FEDERAL AVIATION ADMINISTRATION

INFORMATION SYSTEM SECURITY
TECHNOLOGY OVERVIEW

Version 2.0

September 30, 2002

Prepared by
The MITRE Corporation
for
the Office of Information Services

Acknowledgements

The persons listed below contributed to the research, writing, editing, and production of this document. Their participation was part of a true team effort, and each person's contribution is greatly appreciated.

From the MITRE Corporation:
Eric E. Bloedorn
Chris Clifton
Edwin R. Coover
Donald R. Dobeasky
Gary Forman
Joyce M. Forman
Theodore R. Gobble
Susan V. Gogos
Madge B. Harrison
Carolyn M. Johnson
Paul M. Kellam
Richard D. Murad
Fidel A. Parraga
Theodore L. Signore
Joseph M. Veoni
David M. Wilburn

From the Federal Aviation Administration:
Ernest Lucier, AIO-4
Marshall Potter, AIO-4

Executive Summary

One of the fastest growing areas in information technology (IT) is that of information systems security (ISS). This development is in response to the increasing number and types of computer and network threats, and the growing recognition of operational vulnerability if the necessary IT resources are not available in a satisfactory form for conducting business.

Nowhere is this more important than for the National Airspace System (NAS). The NAS operates 24 hours a day, 365 days a year, managing as many as 20,000 scheduled flights per day. The NAS infrastructure is almost totally information-centric [1]. The IT resources that support the NAS must be available to authorized users at all times and must provide data that can be relied on completely for the safe and efficient management of air traffic.

This document provides a snapshot-in-time overview of ISS technologies in today's marketplace. The information in this overview is to assist FAA personnel responsible for making decisions about requirements, selection, implementation and/or use of ISS products, as well as provide a list of ISS research ideas not being addressed in industry research and development (R&D).

Principal Conclusions

1. **No current single ISS technology will, by itself, provide sufficient protection from current IT threats.** Today's complex IT systems require an appropriate combination of ISS services and functions. Sometimes called Defense in Depth, the FAA characterizes this combination as five reinforcing layers of system protection: Personnel Security, Physical Security, Cyber Hardening of System and Network Elements, Compartmentalization, and Redundancy. This approach is described in Section 1 of the document.

2. **Many of the technologies presented in this document are available for near-term use in the FAA.** To the extent that the FAA's ISS requirements can be met by the current marketplace, the FAA can take advantage of the R&D being spent in response to the larger, government and private sector, customer base. This strategy may be **particularly useful in the case of FAA administrative systems**, whose operations more closely resemble those of the larger customer base. Fourteen ISS technologies are summarized briefly below, and presented in detail in Section 2.

3. **The FAA's NAS operations, however, have requirements that may not be met by the current general ISS technology marketplace. These requirements are unique in their operational nature and possibly their scale. It is toward these requirements that the FAA should focus its ISS R&D efforts, influence, and funding.** Six candidate areas for FAA ISS R&D efforts are summarized briefly following the summary of ISS technologies, and presented in detail in Section 4.

Fourteen ISS Technologies

The following ISS technologies are described in Section 2, grouped within five technology areas that correspond to the FAA's five reinforcing layers of system protection. Most ISS technologies support more than one technology area. The Section 2 descriptions include strengths, issues, selection considerations, contact information, etc.

1. Technology Area: Authentication

- Biometrics: This ISS technology uses physiological or behavioral characteristics to distinguish one person from another. This is a rapidly changing technology and marketplace, with much active research underway. Biometrics can strengthen security when combined with another ISS technology, but most individual biometric technologies do not yet live up to their expected potential or marketing hype.

- Smart Cards: These credit-card size devices provide a convenient, flexible and upgradable platform for several ISS technologies, such as photographs, biometrics, barcodes, magnetic stripes, etc. Smart cards can be used to authenticate the card carrier and to provide both physical and logical access to facilities and IT resources. While tamper resistant, smart cards are not tamper proof, and consequently have significant operational and data privacy concerns.

2. Technology Area: Access Control

- Firewalls: Firewalls consist of systems of hardware and software that can control the flow of traffic between two or more networks or segments of networks. A firewall architecture that is properly configured and maintained can provide good security from external threats. Issues include possible performance bottlenecks, insider attacks, "back door" vulnerabilities, configuration difficulties and cost.

- Intrusion Detection Systems (IDSs): IDSs are software and hardware devices that automate the monitoring of events occurring in a computer system or network, and dynamically analyze them for signs of security problems. Effectively used with firewalls and vulnerability analysis, IDSs provide dynamic monitoring and alerts of suspicious events, and can respond with specific, designed actions. IDS issues include scalability, manageability, interoperability, error rates, downtime and degraded network performance from IDS logging activities.

- Malicious Code and Virus Detection Systems: There are two complementary virus detection systems: anti-virus and behavior-based. Anti-virus software, which is a relatively mature technology, scans a computer's memory and disk drives for the presence of viruses, known by their "signatures." This reactive detection can help contain damage, but systems are vulnerable to new viruses until the signature files have been updated. Much of the new R&D in the area of virus detection is directed toward the newer behavior-based systems, and it appears that organizations may shift to these newer systems in the next few years. Behavior-based systems are proactive and are used when a virus is active to limit the behavior or access of the executable code. These systems implement policies, such as for mobile code, to protect IT resources. Because behavior-based systems are not signature-based, they do not require on-going signature updates, and they provide protection in the time gap between new viruses and signature updates.

- Mobile Code Defense: Mobile code is code that is sourced from a remote, and possibly untrusted, system, such as small applications (applets) downloaded from the Internet. The technical defenses involve various approaches of examining inbound code and deciding what that code may do or access. Being able to tell in advance whether a mobile code unit will attempt to do harm or not is a difficult problem that requires more research. In view of that, organizations must develop strong security policies to protect the IT resources that could be damaged by malicious mobile code.

3. Technology Area: Confidentiality

- Encryption and Cryptography: Cryptography is the science and technology of establishing or protecting the secrecy, authenticity or integrity of data that might be accessed by unauthorized parties. Cryptography uses a body of enabling technologies, including encryption, to facilitate security functionality and objectives. Cryptographic techniques are extremely powerful and useful in enabling security technologies. However, these techniques are difficult to grasp and incorrect decisions may create large risks. Other issues include the strength of the algorithms, key distribution and management, standards and the compatibility between algorithms and implementations from different vendors, product quality, and patent and trademark. Cryptography is a specialized ongoing R&D area.

- Virtual Private Networks (VPNs): Using a blend of security technologies, including encryption, a VPN creates a secure "tunnel" for communicating privately across a shared or public network. VPNs provide a very flexible and cost-effective means for secure, private communications without leasing or managing dedicated lines. However, there are issues of scalability, interoperability and performance degradation. Since VPNs combine various security technologies and products, VPN research is being conducted in each of those components. A key VPN-specific research is that of parallel VPNs to perform load-balancing and provide backup.

4. Technology Area: Integrity and Non-Repudiation

- Logging and Auditing: Logging and auditing are among the most elementary and oldest practices to recover from accidental misuse and malicious intrusions of computer systems. Their very presence can sometimes serve as a deterrent. While still reactive and after-the-fact, today's logging and auditing tools have greatly increased capabilities of data collection and reporting. The massive amounts of data that are, and can be, collected create issues of storage space and difficulty of analysis, some of which can be overcome by exploiting IDSs and data mining tools. There is no notable R&D in logging and auditing per se, but it benefits from research in the areas of pattern recognition, data mining and anomaly-based intrusion detection.

- Data Mining for Intrusion Detection: Data mining evaluates data without previously formulated hypotheses in order to discover or gain new insights that might not be apparent from traditional examination or analysis. Data mining has strong data reduction and discovery capabilities, and can be used to evaluate IDS and logging and auditing data. The potential may be there for data mining to move from being a post-event reactive tool to one with predictive capability. However, data selection, preparation, and accuracy, along with computing time and costs, are issues that must be overcome to reach that potential.

- Public Key Infrastructure (PKI): PKI is a set of ISS infrastructure components, services, policies and procedures dedicated to managing keys and public key certificates to provide security services for enterprise resources. The use of public keys creates flexibility because secure communications can take place without prior arrangement. Key management is a considerable effort, and the development and management of the necessary infrastructure for PKI is still a significant challenge.

5. Technology Area: Availability

- Denial of Service (DoS) Defense: DoS attacks send large numbers of meaningless packets of data to a target system, such that the target system is flooded with so much traffic that legitimate traffic is slowed or halted, i.e., denied. Once an attack has started it is very difficult to stop, and so long as any connecting network has vulnerabilities, then opportunities are available for launching DoS attacks. For prevention, security best practices provide one first line of defense, such as password and configuration management. Filtering software, well-configured firewalls, and IDSs can also help defend against attacks or identify when one has begun. In turn, DoS defense should benefit from research in those three technologies.

- Disaster Recovery and Contingency Planning: Disaster recovery and contingency planning are essential for mitigating the impact of a disaster or to prevent it from happening in the first place. Much of a disaster recovery planning initiative is common sense, and the rest can be greatly simplified through simple-to-use tools and templates. There are many resources available for obtaining guidance and direct support, and a peripheral benefit is a better understanding of the organization. This effort does require continual evaluation, revision, and testing to meet its intended goals.

- Vulnerability Assessment: Vulnerability assessment is a discovery process to try to identify weaknesses in a system's security scheme in order to reduce or better manage any associated risk. Vulnerability assessment is usually performed on a periodic basis, using either host-based or network-based software "agents" that will assess and provide a snapshot of the risk level, but only of the systems or networks where the agents are installed. The type and level of information can vary, but it generally provides a good overview of the state of a system or network. R&D for improved vulnerability assessment tools is an active research area.

Six Candidate Areas for FAA ISS R&D

1. Architecture: This R&D area would address the possibility of an integrated but non-monolithic NAS architecture that would support visual identification of possible ISS attacks, compartmentalization of areas under attack, dynamic reconfiguration, graceful shutdown with reliable recovery, and classification of different ISS requirements in different architectural components.

2. Aircraft Communications and Security: This R&D area would address aircraft communications models that might meet the requirements of timeliness, confidentiality, authentication, and integrity, all within the constraint of limited bandwidth, and still be cost-effective.

3. Public Key Infrastructure (PKI): This R&D area would look for ways to provide a PKI that is based on public key cryptography, but does not use a full certificate-based system; this approach is proposed due to the difficulties and expense of source authentication and signing of a certificate of authenticity.

4. System Security Engineering: This R&D area would examine approaches to "design in" ISS, including identification of security requirements, architecture, design, testing, implementation, operations, and maintenance. This R&D would build on the FAA's ongoing research activity to apply the Common Criteria and the Protection Profile methodology to the security engineering of large IT systems.

5. ISS Technology Performance Considerations: This R&D area would examine a variety of performance considerations related to the operational impact to the FAA's mission, and use of ISS technologies.

6. Staffing Constraints: This R&D area would examine ways to deploy ISS technologies in a way that does not rely on large number of highly skilled ISS technical staff; the research should include requirements for diagnostic tools and optimal architectures and configurations vis-à-vis needed staffing.

ISS Technology Insertion

Technology insertion sometimes focuses on predicting when a technology will be available for insertion into a particular environment. The environment in this case is the FAA, whose operational and mission support environments are changing through modernization efforts. Along with these changes are the increases in the number and types of ISS threats and the corresponding technologies to defend against them.

Since most of the ISS technologies discussed in this document have commercially available products in today's marketplace, the question is not so much *when* to insert the technology based on the state of the technology. Rather the question is when will the FAA be ready to insert one or more ISS technologies *based on requirements.* Since each of these technologies is evolving, each at its own pace, the approach should be to select the best set of ISS technologies to achieve a particular goal, and expect to upgrade or refresh them in the future.

Proposed Next Steps

In order for the FAA to take advantage of the work in this document, the following four steps are proposed, and discussed in further detail in Section 5:

1. Disseminate this information to all FAA Lines of Business to assist with ISS technology decisions.
2. Define and champion FAA-specific ISS R&D whose requirements will not likely be met by the commercial marketplace.
3. Develop an ongoing Layered System Protection program that includes ISS threat identification, funding strategies, and well-crafted implementation plans.
4. Maintain and update this type of ISS information to keep it useful.

TABLE OF CONTENTS

Page

1. Introduction

One of the fastest growing areas in information technology (IT) is that of information system security (ISS). This development is in response to the increasing number and types of computer and network threats, and the growing recognition of operational vulnerability when the necessary IT resources are not available in a satisfactory form for conducting business.

Nowhere is this more important than for the National Airspace System (NAS). The NAS operates 24 hours a day, 365 days a year, managing as many as 20,000 scheduled flights per day. The NAS infrastructure is almost totally information-centric [1], and the IT resources that support the NAS must be available to authorized users at all times and must provide data that can be relied on completely for the safe and efficient management of air traffic.

1.1 The FAA's Layered Approach to ISS

The Chief Information Officer (CIO) of the Federal Aviation Administration (FAA), Dr. Daniel J. Mehan, recently contributed a paper to the ISS section of *Transportation Research News* (November-December 2000) entitled "The Federal Aviation Administration's Layered Approach" [1]. In that paper, he characterized the FAA's ISS structural model as a notional pyramid with five reinforcing layers of system protection. (Section 2 will describe this model in detail.) This model was subsequently expanded in an article by Dr. Mehan and Marshall Potter, Chief Scientist for Information Technology at the FAA, "Building Trustworthy Systems: An FAA Perspective" [3].

The layers of this model can be mapped (See Section 2.) to five major Technology Areas of security services/functions as defined by the International Organization for Standardization (ISO) Security Reference Model. These ISO-defined security services comprise the following: Authentication, Access Control, Confidentiality, Integrity, and Availability. (For completeness, the Non-Repudiation security service is also included and has been placed in the Integrity layer.)

While all five of the security services are important to the successful operation of the NAS, the FAA often considers data integrity and availability among the most important.

1.2 Purpose of This Document

The purpose of this document is:

- To serve as a reference for Integrated Product Teams and other organizations that need information about ISS technologies
- To assist the FAA's AIO-4 organization in some of its decisions of expending resources for ISS research and development (R&D)

- To provide a snapshot of the current state of the five Technology Areas and their supporting ISS technologies and products
- To provide a compilation of current and, where possible, future R&D in the five ISS Technology Areas
- To provide references to more specific, and perhaps more current, information about ISS products, R&D, and sources. Because all of these technology areas are changing quickly in response to new and different security threats, the reader is encouraged to utilize those references for additional information.

1.3 Audience for This Document

The intended audience for this document is the FAA personnel responsible for making decisions about requirements, selection, implementation and/or use of ISS products. This document may be of particular use, for example, to persons responsible for compliance with FAA Order 1370.82, *Information Systems Security Program* [2].

Other audiences for this document may include any persons with a general interest in the current state of ISS technology and related R&D.

1.4 Role of Best Practices

Best practices -- those technologies and procedures widely adapted by industry -- play several key roles in ISS:

- Helping to avoid serious mistakes: An individual organization can benefit from the knowledge and experience of other, especially similar, organizations, as well as from information provided by technology market researchers. ISS decision making in a fast-changing technology environment is difficult and not necessarily perfect. However, the generally accepted best practices that have resulted from the experience of other organizations can provide guidance to at least help avoid likely major pitfalls.

- Helping to make better decisions: The other side of the coin is to benefit from successful experiences or choices of other organizations, especially where the circumstances indicate possible success in another organization.

- Leveraging ISS technology investments: In order to obtain the maximum benefit from ISS technology investments, appropriate management and infrastructure elements, such as policies and procedures, must be in place for operational use.   In addition, one particular combination of ISS technologies may be more effective than another. The best practices of other organizations can provide guidance in both the selection and support of ISS technologies.

Three major areas in which best practices can be very helpful are as follows:

- Requirements: One of the primary reasons given for unsuccessful ISS is the lack of solid requirements development prior to selecting and implementing ISS technologies. Before deciding on a specific ISS technology to implement, an organization should develop clear goals and then evaluate the ISS technologies that support those goals. As shown in Appendix A, there are usually several ISS technologies that support different Technology Areas, such as Access Control. An organization should examine the strengths of each corresponding supporting ISS technology and select one or more whose strengths best match the organization's ISS requirements.
- Layered ISS technologies: Each of the ISS technologies presented in this document has strengths and issues. No single ISS technology by itself can provide the level of information security (IS) that most organizations need or want in an increasingly complex information environment faced with an increasing number and kind of threats. The experiences of many organizations have shown that the initial implementation of a single ISS technology will not necessarily lead to success in protecting the organization's information resources. Increasing security usually means adding or layering ISS technologies and not depending on any single one. Another name for this layered approach is "Defense in Depth." Appendix A illustrates possible combinations of ISS technologies that can be used to support different Technology Areas.
- Management of ISS technologies: Once installed, ISS technologies require ongoing management or they will not be able to respond to changing threats. Key management areas are as follows:
  - Configuration: Each ISS technology must be configured properly. For example, an improperly configured firewall may not be effective, and, worse, may provide a false sense of security.
  - User passwords: An organization is vulnerable if its user passwords are not strong. Strength of passwords is inversely related to how easily and quickly a hacker can determine a valid password. Once the hacker has a valid password, he/she can have access to the information resources of that user. Examples of weak passwords are proper names, date of birth, and words that can be found in a dictionary lookup or generated randomly with little effort. Examples of strong passwords are those with a mix of alphanumeric and special characters in a random pattern.
  - System passwords: System software comes with a default password known to the system installers – and often to hackers. System passwords should be changed as soon as the system software is installed.
  - Maintenance: As threats change, ISS vendors provide periodic updates, for example, to virus detection software. Organizations must apply these updates as soon as possible, because their information systems are vulnerable to the new threats until the updates are applied.

1.5 ISS Technology Insertion

Technology insertion sometimes focuses on predicting when a technology will be available for insertion into a particular environment. In this case, most of the ISS technologies discussed in this document have commercially available products in today's marketplace. Each of these technologies is developing in response to market demand, and each technology has its own set of strengths and issues. The question is not so much *when* to insert the technology based on the state of the technology. Rather the question is when will the FAA be ready to bring one or more ISS technologies into its environment *based on requirements.* Since each of these technologies is evolving, each at its own pace, the approach should be to select the best set of ISS technologies to achieve a particular goal, and expect to upgrade or refresh those technologies in the future. In this kind of evolving situation, the same kinds of questions should be asked as when acquiring any new technology: how closely the product meets requirements, robustness of product, track record of product, compliance with standards, and stability/viability of vendor.

The key to successfully introducing new technologies into an environment is high quality requirements development. An organization should not decide, for example, to use encryption without first understanding the problem being solved, then developing requirements, and after that determining whether encryption is one of the technologies to solve the problem. In addition, since none of the current ISS technologies by itself will provide 100% security, organizations should plan to use more than one ISS technology to attain stronger information assurance.

In addition to ensuring that a specific ISS technology is a good fit to meet functional requirements, an organization should also take into consideration the maintenance and operational aspects of the technology. This consideration should clearly include the direct costs for items such as upgrades but also the staffing implications to perform maintenance, especially for newer products when fewer technical staff may be available in the marketplace.

1.6 Organization of This Document

This document is framed by Dr. Mehan's initial article [1] and the later article by Dr. Mehan and Marshall Potter, [3] and presents material grouped by the five Technology Areas that correspond to the FAA's five layers of system protection.

- Section 2 describes each of the five Technology Areas and, for each area, presents the current state of one or more technologies, including both products and R&D. It is important to note that one technology may support more than one technology area. Appendix A provides a mapping of specific technologies to ISS technology areas, and illustrates the nature of this overlap. For each technology presented, a short discussion is included regarding its possible insertion into the FAA environment.
- Section 3 presents a summary of R&D efforts relative to the ISS Technology Areas.

- Section 4 presents some candidate areas for FAA R&D in ISS technologies. This section discusses ISS requirements that the FAA shares with the larger community of IT users as well as the ISS requirements that are unique to the FAA.

2. ISS Technology Areas

The FAA has developed a structural model to help focus ISS efforts [1]. This model is depicted in the shape of a pyramid in Figure 2.1. In the pyramid, there are five reinforcing layers of system protection. From top to bottom, the layers are: Personnel Security, Physical Security, Cyber Hardening of System and Network Elements, Compartmentalization, and Redundancy.

The top layer, Personnel Security, is designed to ensure that personnel who play a sensitive role or have access to sensitive information are trustworthy.

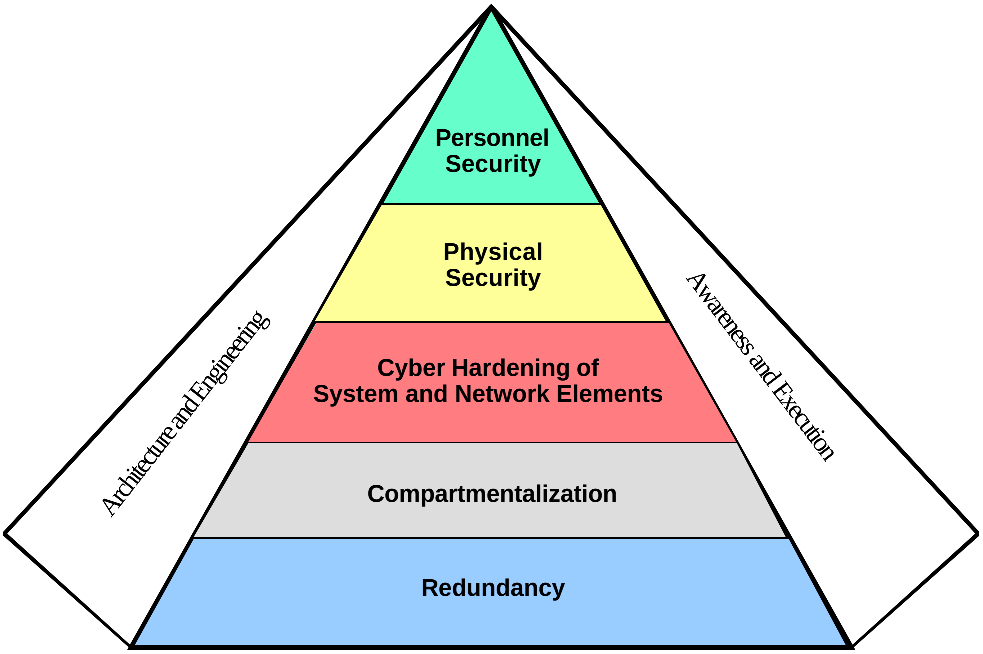

Figure 2.1 FAA's Five Layers of System Protection

The second layer, Physical Security, is designed to ensure that FAA facilities are safe from unauthorized physical access and harm.

The third, or middle, layer is Cyber Hardening of System and Network Elements. This layer refers to improving, or hardening, the security services and functions of all FAA system and network elements, making it more different to knock out individual elements.

The fourth layer is Compartmentalization. The term "compartmentalization" means a mechanism to constrain and control the impact of any single security incident within the ISS model.

The final layer is Redundancy. Redundancy provides a necessary degree of robustness to ensure that FAA systems will do what is expected of them. Through Redundancy the occurrence of single points of failure are reduced.

There are right and left aspects of the pyramid dealing with Awareness and Execution and Architecture and Engineering, respectively. These two sides of the pyramid apply to all the layers.

Relative to the five layers of system protection there is a corresponding model of "ISS Technology Areas." From the top to bottom these ISS Technology Areas are Authentication, Access Control, Confidentiality, Integrity/Non-repudiation, and Availability. The relationship of the ISS Technology Areas to the FAA's layered model is shown in Figure 2.2. Each of these areas is described in the sections that follow.

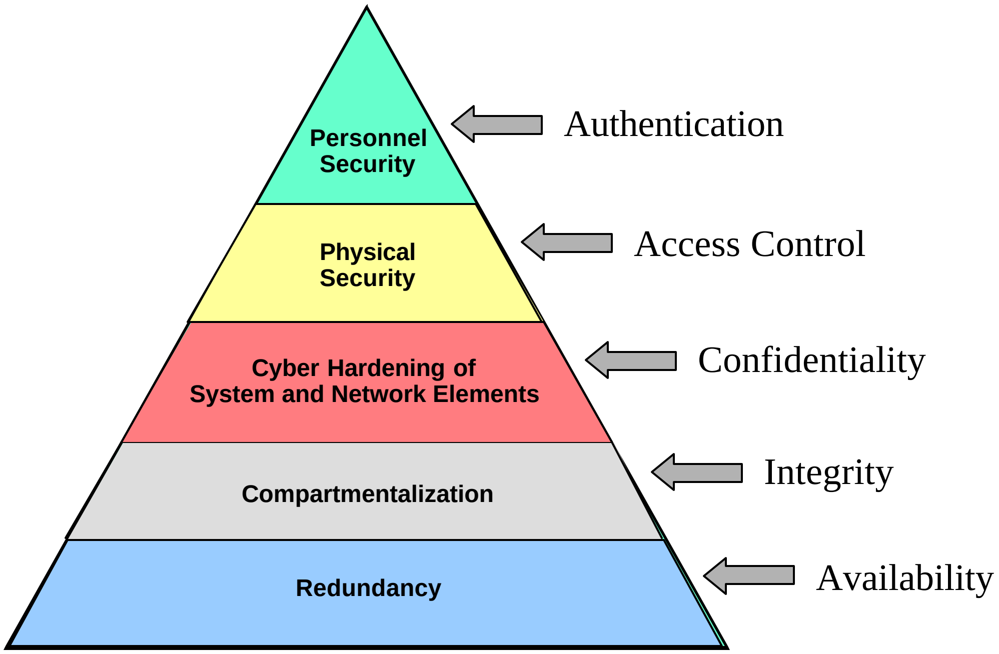

Figure 2.2 Relationship of the ISS Technology Areas to the Layered System Protection Model

For each of the five ISS Technology Areas shown in Figure 2.2, there are several ISS technologies that support the area. These technologies are shown in Table 2.1 and mapped to the ISS Technology Areas they support. This presentation is to illustrate that more than one ISS technology may be used to support any one Technology Area, and suggests which ISS technologies might be used in combination to strengthen ISS support. Technologies may be, and often are, used in combination to strengthen the ISS support for a specific Technology Area.

Table 2.1 FAA ISS Technology Areas and Supporting ISS Technologies

FAA ISS Technology Areas >>	Authentication	Access Control	Integrity/Non-repudiation	Confidentiality	Availability
Biometrics	X				
Data Mining		X			
Denial of Service (DoS) Defense		X			X
Distributed DoS Defense		X			X
Disaster Recovery and Contingency Plan					X
Encryption (and Cryptography) - Hardware and Software	X	X	X	X	X
Firewalls	X	X			
Hostile Code Detection		X	X	X	
Intrusion Detection Systems		X			
Logging and Auditing			X		
Malicious Code and Virus Detection		X	X		
Mobile Code		X	X		
Public Key Infrastructure (PKI)			X		
Smart Cards	X	X			
Virtual Private Networks (VPN)	X	X	X	X	
Vulnerability Assessment					X

2.1 ISS Technology Area 1: Authentication

Authentication verifies the identity of a principal. Authentication establishes the validity of a transmission, message, or originator, or it serves as a means of verifying an individual's authorization to receive specific categories of information.

In the FAA environment, authentication must ensure that personnel who play a sensitive role or have access to sensitive information are trustworthy and have an operational need for access to that information. This is a cornerstone to having data and information that can be trusted for NAS operations.

2.1.1 Biometrics

Biometrics refers to technologies for measuring and analyzing human body characteristics, especially for authentication purposes. These technologies take advantage of the fact that certain physiological characteristics (e.g., fingerprints) and behavioral characteristics (e.g., written signature) reliably distinguish one person from another. The statistical analysis of these characteristics can be used to create a unique identifier in the form of the digital representation of the characteristic. With this, biometrics works to provide improved identification and authentication processes.

The security field uses three different types of authentication:

- Something you know: a password, personal identification number (PIN), or some personal information such as your mother's maiden name
- Something you have: a card key, smart card, or token
- Something you are: a biometric

There are two kinds of biometric systems: identification and authentication. Identification is also called recognition or open search. Authentication, or verifying a claimed identity, is also called verification or closed search.

The majority of biometric devices operate in authentication mode. Initially, an individual “enrolls” in the system to be used by providing a sample, such as a facial or iris scan, handprint or fingerprint, or voice sample. The biometric system captures the sample and converts it into a digital sample that is stored as a template for that user. Once enrolled, the individual makes a claim of identity by presenting, for example, a PIN or a machine-readable identification card. The biometric device captures a live biometric sample and compares what the user has presented with the stored template of that user's characteristic. This is a simple and straightforward operation, with a one-to-one match.

A few biometric systems offer biometric identification. In these systems, the user makes no claim to identity, but submits a live sample, such as a facial scan or voice sample, and the system attempts to identify the individual with a database of templates. This is a more complex one-to-many match that may generate a multiple result according to the number and similarity of stored templates. This mode is more challenging, time-consuming, and costly than the authentication mode. For now, this works well from a performance standpoint if the database of stored templates is relatively small.

Current Strengths

- Availability: Since these characteristics are tightly bound to the person, they cannot be lost, stolen, forgotten, or loaned. They are always available to the person.
- Enabling: Positive identification of users allows high-value communications-based transactions to be offered, along with improved accountability in audit trails.
- Reduced cost in related areas: Password management and related overhead costs can be reduced.

Current Issues

- System cost: There is a large variance in the cost of the different technologies. The cost of some technologies is still high, but others have experienced significant cost declines during the past year.
- Privacy: Privacy concerns, especially of consumers, result in opposition to biometrics.
- Personal concerns: Opposition to biometrics is also caused by a variety of personal concerns, such as the stigma of fingerprinting and its criminal connotation, hygiene with the use of a hand geometry scanner and retina scan, and the possibility of actual harm from retina scans where light is shone into the eye.
- Errors: Time and environmental conditions cause errors that affect biometric data, either directly or by interfering with data collection.
- Accuracy: Biometrics have an error rate that still needs improvement. Biometrics are rated by two interdependent methods: false-acceptance rate and false-rejection rate. Ideally, both of these rates would be zero, but parameters can be used to manage the rates to the goals of the organization.
- Compromised traits: A biometric trait cannot be reissued. If a biometric trait is compromised, the original owner/user can no longer use that trait on that system, or any similar system, for life.

Ongoing R&D

Research is ongoing in all areas of biometrics. The names and contact information for the current major research centers are shown in a list maintained by Purdue University at the following Uniform Resource Locator (URL) on the World Wide Web (WWW, or Web):

http://www.cerias.purdue.edu/coast/hotlist/education/research_centers.html

Leading Organizations

In addition to the research centers indicated earlier and the vendors listed below, there are several general resources available in biometrics.

International Biometric Industry Association (IBIA), http://www.ibia.org: The IBIA focuses on educating lawmakers and regulators about how biometrics can help deter identify theft and increase personal security. The IBIA is open to biometric manufacturers, integrators, and end users.

The Biometrics Consortium (BC), http://www.biometrics.org: The BC serves as one of the U.S. Government's focal points for research, development, testing, evaluation, and application of biometric-based systems. More than 60 different federal agencies and members from 80 organizations participate in the BC. The BC's web site and its open listserv are two of the consortium's richest resources.

Association for Biometrics (AFB), http://www.afb.org.uk: The AFB's goal is to promote the awareness and development of biometric-related technologies. It provides an international forum for R&D, system design and integration, application development, market development, and other issues.

Avanti, http://homepage.ntlworld.com/avanti/: Avanti is a reference site for biometrics. Avanti contains a considerable amount of background information about biometrics, their use in everyday business situations, and how to deploy them.

Biometrics: Journal of the International Biometric Society: This is a quarterly publication that promotes and extends the use of mathematical and statistical methods in various disciplines.

Product/Technology Status

Biometrics is an emerging technology area with around 600 products currently available in the marketplace. The 1999 revenue of biometrics companies was estimated at $166 million, and it is predicted that this will increase to $1.8 billion by 2004 [4].

Various organizations are involved in evaluating existing products, some of which are listed below:

Organization	Contact Information
DoD, Biometrics Fusion Center	(Note: There are no plans to release the test findings.)
Biometrics Consortium	Jeff Dunn: Dunn@biometrics.org Telephone: 301-688-0293
National Institute of Standards and Technology (NIST)	▪ P. Jonathon Phillips: jonathon@nist.gov ▪ C. L. Wilson: cwilson@nist.gov ▪ Mark Przybocki: mark.przybocki@nist.gov

Organization	Contact Information
Performance Testing of Biometric Systems National Physical Laboratory	Tony Mansfield: tony.mansfield@npl.co.uk
Performance assessment of a face-verification based access control system University of Manchester, United Kingdom (UK)	Gavin Wheeler: gavin.wheeler@man.ac.uk
Comparative Study of Biometric Identification Systems	• Zwiesele, BKA, Wiesbaden (Federal Criminal Investigation Office of Germany) • Munde, BSI Bonn (German Information Security Agency) • Dr. C. Busch, H. Daum, IGD Darmstadt (Fraunhofer Institute of Graphical Data Processing)

Current Technologies Grouped As Six Submarkets

1. Finger scan: This technology looks at the patterns found on a fingertip. This is the largest and strongest sector of the biometrics technology market; a greater variety of fingerprint devices are available than for any other biometric. Despite the common-criminal stigma of fingerprinting, users have found this to be the most acceptable form of biometrics technology. The two problems encountered with this technology are unreadable fingerprints and mobility of the scanning device.

   Leading companies for this technology and their submarket share are [4]:

   - Identix (27% of submarket share): www.identix.com
   - Sagem (23%): www.sagem.com
   - Veridicom (12%): www.veridicom.com
   - Infineon (11%): www.infineon.com

2. Voice authentication: Voice authentication is based on voice print authentication in which the technology is able to transform voice into text. The most popular current application of this technology is voice-automated dialing, but the expectation is that it will be improved and used for authentication purposes. The advantage of and potential for this technology is that no new hardware is required for authentication through Personal Computers (PCs) that already contain a microphone. However, poor quality and ambient noise reduce the effectiveness of verification, and the related software needs improvement.

   Leading companies for this technology and their submarket share are [4]:

   - T-NETIX (30%): www.t-netix.com
   - ITT (26%): www.itt.com

- Nuance (15%): www.nuance.com
- Veritel (11%): www.us.veritel.com

3. Signature verification: This technology analyzes the way a user signs his/her name. A handwritten signature is converted mathematically into an electronic digital signature that serves as a form of encryption authentication using a digital image of the signature. This technology requires a stylus and a touch pad on which the user physically signs in. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. User acceptance is good for this technology because signatures are already used as a means of transaction-related identity verification, and the technology is a logical extension of that process.

   Leading companies for this technology and their submarket share are [4]:

   - Communication Intelligence Corporation (CIC) (26%): www.cic.com
   - Cyber-SIGN (23%): www.cybersign.com
   - PenOp (21%): www.penop.com

4. Facial scan: This technology analyzes facial characteristics. For network authentication purposes, this technology is considered to be a niche market because of the need for an extra peripheral—a digital camera to develop a facial image of the end user—that is not customarily included in basic PC packages. If digital cameras are embedded in more devices in the future, this submarket will likely grow. One current application of this technology is a facial database of scam artists for quick detection by casino security personnel.

   Leading companies for this technology and their submarket share are [4]:

   - Visionics (43%): www.visionics.com
   - Viisage (24%): www.viisage.com
   - eTrue (10%): www.etrue.com

5. Eye scan: This technology is similar to facial scan, but a camera takes a picture of the eye, specifically the iris, instead of the face, requiring the eye to be at close proximity to the camera. The end user regards this technology to be invasive, thus, there is some opposition to its use. This technology is expected to grow because of its accuracy, and its ability to authenticate the 3-4% of the population with unreadable fingerprints.

   There is one major vendor [4]: Iridian (67%): www.iriscan.com

6. Hand/finger geometry: This technology involves analyzing and measuring the shape of the hand. This technology is used primarily for physical access authorization and time attendance recording. It offers a good balance of performance characteristics and is relatively easy to use. There is some opposition to its use for hygiene reasons. It is not generally used for network authentication.

There is one major vendor [4]: Recognition Systems (75%): www.recogsys.com

Technology Selection Considerations

1. Criteria that could be used to evaluate and compare biometric technologies:

- ROC (Receiver Operator Characteristics) curves:
  - False Accept Rates (FAR) or "false accepts"
  - False Reject Rates (FRR) or "false rejections"
- Ability to set or adjust decision threshold (FAR and FFR tradeoff) based on goals of organization
- Failure to acquire rates
- Enrollment time
- Throughput rate (average transaction time for matching), especially for large data bases
- Life cycle cost (acquisition, integration, maintenance, upgrades, training, management, etc.)
- Environmental, operational or usability issues,
  - Environmental restrictions, limitations, hindrances
  - Scalability, especially for use with large data bases
  - Integration with other operations or policies
  - User acceptance
- Business process, policies needed
  - Management of enrollment
  - Administration of data
  - Policies for collection and use
- Known vulnerabilities for each biometric technology
  - Mimic attacks, disguisability, spoofability
  - Counter measures (liveness testing)

2. Current performance considerations:

- The biometric technology market is changing rapidly, standards are not widely supported, and there are not clear thresholds such as with some other technologies. In addition, degree of performance can vary based on the operational environment, such that test results may not generalize well across applications or across different environments.

- Of special consideration, however, is the true life cycle cost of a biometric technology, including enrollment, integration and maintenance, technology refresh, training, management of the data, and development of supporting policies. Integration effort can be signification if biometric authentication is used to control access to disparate electronic resources such as operating systems, networks, databases, and web sites.

3. Evaluation and testing considerations:

    - Any evaluations and selections should be within the context of any FAA-wide standards and any FAA smart card efforts that include biometrics.

    - FAA should follow closely the independent evaluations about all biometric technologies. The biometric market is changing frequently in terms of new products and performance of products. Many products do not yet live up to the hype. Any testing and evaluation must take into account performance under a variety of operational conditions. If deployment is expected on a large scale, testing must be done to ensure that the product performs within its stated threshold on that scale.

    - The FAA William J. Hughes Technical Center and the FAA AIO organization could conduct or assist with the testing and evaluation. The AIO organization is in the process of testing some biometric technologies at the time of this writing.

Technology Insertion

The biometric technologies should not be used as single technology solutions. Rather they should be used in combination with other ISS technologies to strengthen the information assurance needed. The biometric technologies that have proven to be effective, such as fingerprints, handprints, and iris scans, can be inserted into the FAA environment when the requirement is there. Other biometrics, such as face scanning, have not reached a high confidence level, and the FAA should wait for the marketplace to respond.

Future of Biometrics

For the future, there are some trade-offs of convenience versus the strength of the authentication. Convenience technologies include multifunctional devices that are capable of doing more than simple end-user authentication, such as digital cameras for facial scan and microphones for voice authentication. Single-function devices, such as fingerprint scanners, may fare better if market demand moves to devices that offer stronger authentication.

It is not clear how the biometrics market will be affected by pending decisions regarding privacy, security, or other legislation ratified by the U.S., the United Nations, the European Union governments, or Japan.

Because of the error rate and reliability issues from using a single biometrics technology, it appears likely that multifactor authentication will increase, especially in the business arena.

Standards are emerging to provide a common software interface, to allow sharing of biometric templates, and to permit effective comparison and evaluation of different biometric technologies.

Future Biometric Technologies

- Body odor: This technology digitally records body odor for identification. The system being worked on by Mastiff Electronic Systems, of the UK, is still very expensive (about $50,000), and is years away from commercial release.
- DNA matching: This technology can provide proof-positive identification of an individual, except in cases where individuals, such as identical twins, share a genotype. However, this identification process is intrusive, and takes too much time for “on the spot” identification.
- Keystroke dynamics: This innovative technology is also referred to as typing rhythms. Two distinct variables are measured: “dwell time,” the length of time a user holds down a particular key, and “flight time,” the length of time it takes a user to move between keys.
- Palm print: This technology analyzes the pattern of lines on an individual's palm much the same as fingerprints.
- Vascular patterns: This technology analyzes the pattern of veins on various parts of a person's body, including the wrist, the back of the hand, and the face.

2.1.2 Smart Cards

Smart cards are multipurpose security devices that can be used for access control, authentication, privacy protection, and other applications. The smart card, or intelligent token, is a credit-card sized, tamper-resistant security device embedded with an integrated circuit chip (ICC) for information storage and information processing. It provides not only memory capacity, but computational capability as well.

There are two types of smart cards: intelligent smart cards and memory smart cards. Intelligent smart cards have the ability to make decisions, and to store and secure data; they also use read/write capabilities. Memory smart cards are used only for information storage, such as long-distance phone charges, retail transactions, and vending applications.

The self-containment of a smart card makes it resistant to attack, as it does not need to depend upon potentially vulnerable external resources. Because of this characteristic, smart cards are often used in applications that require strong security protection and authentication. Examples of smart card applications are use as an identification card, medical history card, or credit/debit bankcard. All of these applications require sensitive data to be stored in the card, such as biometrics information of the card owner, personal medical history, and cryptographic keys for authentication. Smart cards can be used together with other security technologies, such as asymmetric cryptographic algorithms and biometrics identification, to provide highly assured and trusted applications.

The capability of a smart card is provided by its ICC. A schematic diagram of a smart card is shown in Figure 2.3. Typically, an ICC consists of a microprocessor, read only memory (ROM), non-static random access memory (RAM), and electrically erasable programmable read only memory (EPROM), which will retain its state when the power is removed. The current circuit chip is made from silicon, which is not flexible or easily broken. In order to avoid breakage when the card is bent, the chip is restricted to only a few millimeters in size.

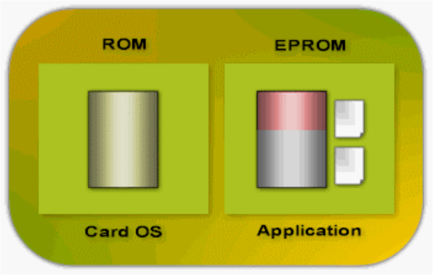

Figure 2.3 Schematic of Components Within a Typical Smart Card

Current Strengths

- Access Control: By establishing identity, a smart card enables the verification of a cardholder's identity to permit access to physical sites, networks, individual computers and accounts.
- Relationship Management: By enabling an online link with issuer-held customer data (i.e., similar to a magnetic stripe credit or debit card or a user name/password combination on an Internet site) or the reading of descriptive identity from the card itself, initiatives such as differentiated servicing, targeted marketing, and loyalty point programs can be enabled.
- Transactional Record Keeping: By retaining a record of usage on the card itself, record keeping is enabled by the cardholder (or the cardholder's organization, in the case of corporate use).
- Convenience: Smart cards can provide convenience to end users by:
  - Streamlining access to goods and services (e.g., transportation access cards that enable drivers to bypass toll lines).
  - Eliminating remembered passwords and PINs through biometric identification cards. (However, remembered PINS will increase in comparison to magnetic stripe cards when biometrics are not used.)
  - Consolidating passwords and PINs by storing them on the cards.
  - Reducing the need to complete redundant forms because of the capability to prepopulate online order forms.

- Renewability: Smart cards are a renewable security element. Their cryptographic keys and/or algorithms can be changed as required. For instance, if a particular cryptographic algorithm is compromised, then a back up algorithm in the card could be activated. Smart cards generally are replaced within 2-3 years, at which time new countermeasures can be incorporated during the renewal process.

- Certificate location and key generator: The advantages that the smart card has over other hardware as a certificate location and key generator are as follows:

  - Extensive security features engineered into its semiconductor chip
  - Low-cost production
  - Ease of integration with other hardware platforms or multifactor authentication solutions

- Others: Other advantages of smart cards are as follows:

  - Multiple services can be provided with one card
  - Paperless environment
  - Organized information
  - Fraud reduction

Current Issues

- Costs: There are additional costs for installing card readers and software on all client machines. There are development costs for proprietary program interfaces for both client and server machines for particular applications. In addition to developmental and hardware costs, there will be increased costs due to fees assessed by the data owner for the use of the data. For any given application, there may be several sources of data, each with different owners; the data owners will usually assess fees for the use of their data.

- Card Readers: Smart card readers are not standard equipment in corporate PCs. And the leading laptop and desktop computer vendors are working very slowly toward offering smart card readers as standard equipment.

- Environmental vulnerabilities: Smart cards are vulnerable to static electricity, magnetic fields, temperature, and ultraviolet light. If the smart card is electronically compromised or physically broken, the smart card is unusable.

- Privacy: Smart cards raise many privacy issues. Tracking the movements of users, storing their private information, and sharing data among data owners (across organizations), all contribute to a lack of user privacy.

- Operational reliability: Reliability of smart cards is a complex topic. Smart cards are tamper resistant, but **not** tamper proof. All manufacturers warrant that their products will pass the ISO reliability tests. Unfortunately, every project has different terminals, software, environmental conditions, and usage patterns, which cannot be completely foreseen or fully tested. Additionally, as more features are added to the card (e.g., magnetic stripe, photo image, smart card chip, embossing, surface printing, proximity technology), it only takes one element to fail for the card to be compromised and unusable.

- Damaged or lost cards or readers: Damaged cards and/or readers present potential difficulties in permitting access to controlled resources. A person who loses or forgets his/her card will temporarily be locked out of systems or physical areas if the card is required for access. It may be infeasible to provide temporary "keys" for users who forget their cards. Broken readers will temporarily prevent all users access unless there is an alternate or backup system in place for access control. When smart cards are used, there is always a need for alternative emergency access to the systems, such as passwords or photo IDs.
- Security infrastructure: Smart card readers for physical access, for example, to buildings or rooms, require separately protected distribution systems. It is relatively easy to break into the wiring of a smart card reader system without being noticed unless such systems are properly equipped with alarms, cameras and steel conduit to protect the cabling from taps.

Ongoing R&D

One source for ongoing research on smart cards is the Electronic Commerce Research Room, http://www.wilsonweb.com/cgi-bin/au/research/money/smart.htm. This web site is primarily focused on e-business transactions and has a pointer to articles and discussions on smart cards. However, a subscription to the *Web Commerce Today* periodical is required for access to the site.

Other security research is being conducted in the Information Systems Security Engineering (ISSE) department of George Mason University, Fairfax, VA, under the leadership of Dr. Ravi S. Sandhu (703-993-1659).

The U.S. Government's web site is a source of all current smart card applications within the Government. As part of the U.S. General Services Administration (GSA) smart card initiatives, the Office of Government-wide Policy (OGP) is attempting to identify various smart card projects and applications pursued by federal agencies to make the Government function more efficiently. This database is the result of OGP's survey of federal agencies completed in August 2000. The purpose of this database is for information sharing, identifying areas of interest, and sharing technology advancement among federal agencies' smart card projects: http://smart.gov.

The GSA has also published *Government Smart Card Technical Interoperability Guidelines (Version 1.0)*, which can be downloaded from the same web site shown above: http://smart.gov. In addition, the GSA has published Smart Card Policy and Administrative Guidelines, which can be downloaded from: http://smart.gov/101800_policy_handbook.pdf.

Leading Organizations

The following table lists some organizations focused on smart card technology:

Table 2.2. Organizations Focused on Smart Card Technology

Smart Card Organization	Internet Address
American Card Technology, Inc.	http://www.amercard.com
Card Europe	http://www.gold.net/users/ct96/
Global Chipcard Alliance	http://www.chipcard.org
International Card Manufacturers Association	http://www.icma.com
SmartCard Developers Association	http://www.scard.org/
JavaCard Forum	http://www.javacardforum.org
Smart Card Industry Association	http://www.scia.org/aboutsmartcards/
The Smart Card Club	http://www.smartcardclub.co.uk/
OpenCard Consortium:	http://www.opencard.org/index-consortium.shtml
Smart Card Resource Center	http://www.smart-card.com/
UCL Microelectronics Laboratory-Crypto Group	http://www.dice.ucl.ac.be/crypto/card.html
SmartCard Central	http://www.smartcardcentral.com/
The SmartCard Forum	http://www.smartcrd.com www.smartcardforum.org

There are hundreds of companies involved in developing smart card applications. There are the ICC smart card manufacturers, smart card software developers (operating systems (OS), applications, access), smart card integrators, and smart card terminal manufacturers. There is no set of companies that dominates the market share for developing smart card applications or appliances. American Express and VISA credit card companies are very motivated in developing smart card applications for the added security, convenience, and cost-savings. Some of the many companies involved in various aspects of smart card technology are listed below:

- 3-G International
- American Express Travel Related Services
- First Access
- Gemplus
- Giesecke & Devrient

- International Business Machines (IBM)
- Toshiba Corporation
- TOWITOKO
- Schlumberger
- Siemens
- Sun Microsystems
- UbiQ Inc.
- Visa International
- XAC Automation

Table 2.3 Points of Contact

Organization	Contact Information
Cambridge University Computer Laboratory, Pembroke Street, Cambridge CB2 3QG	Ross J. Anderson: ross.anderson@cl.cam.ac.uk
ISSE Department, George Mason University, Fairfax, VA	Ravi S. Sandhu: sandhu@isse.gmu.edu http://www.isse.gmu.edu
Prasad's Electronic Commerce & Smart Cards Page	http://home.att.net/~s-prasad/ecsc.htm
GSA Federal Technology Service, Center for Smart Card Solutions	http://www.gsa.gov
U.S. Government	http://smart.gov

Technology Insertion

Smart cards are a proven technology, and the FAA is considering issuing smart cards in the near future for access control at FAA facilities. Smart cards provide a platform for the use of several ISS technologies, which can be placed on the card when their respective maturity levels match the FAA requirements.

Future of Smart Cards

Smart cards have moved beyond much of the R&D phase, and now will be more driven by applications. In the near future, the traditional magnetic stripe card will be replaced by an integrated, multi-application smart card, which is known as an electronic purse (or wallet) in the smart card industry. The smart card is becoming increasingly significant for controlling access to facilities and systems as well as for personal transactions. It will be used to carry sensitive and critical data about the users, which was not possible with the magnetic stripe card. Therefore, there are many issues and controversies regarding the security of smart cards that may impede certain types of applications.

Consumer PCs will not ship with smart card readers as a standard feature until after 2004. It is projected that by the end of 2003, 33 percent of the installed base of corporate Windows 2000 users will use a smart card for PC logon. Through 2006, the majority of smart cards will feature a single application. Any multi-application cards will typically only support services provided by the issuing organization.

2.2 ISS Technology Area 2: Access Control

Access Control prevents unauthorized access to—and unauthorized use of—resources. Access controls are safeguards used to control user access to files, ports, or other system resources. It is normally a fundamental part of an overall defense in depth strategy. Access controls are often inherent in the application or OS software (e.g., setting file access privileges in Unix).

In the FAA operating environment, access controls must ensure that FAA facilities are safe from unauthorized physical access and harm and that access is controlled for the information system resources used in those facilities.

2.2.1 Firewalls

A firewall is a system, or group of systems, that enforces a security policy by controlling the flow of traffic between two or more networks. Firewalls can defend against attacks ranging from unauthorized access, Internet Protocol (IP) address spoofing, session hijacking, viruses and rogue applets, rerouting of traffic, and some denial of service (DoS) attacks.

Traditional firewalls are network based. These firewalls are often placed between an organization's internal network and an external network, such as the Internet. However, firewalls are also used to segment parts of internal networks. As such, they provide both a perimeter defense and a control point for monitoring access to and from specific networks.

Other firewalls, termed "host-based firewalls," typically are used to protect a single system from network-based threats. Most of these programs inspect all incoming and outgoing packets and match them against known attack or intrusion signatures. When an intrusion or attempted attack is discovered, the program will log the attempt and provide an alert.

Firewalls may be packaged as system software, hardware and software combined, and dedicated hardware appliances (easy to configure integrated hardware and software packages that run on dedicated platforms).

Firewalls can control access at the network level, the application level, both application and network levels, and the session level. At the network level, they can restrict packet flow based on protocol attributes, such as source and destination address. At the application level, they may act as intermediaries between source and destination applications and enforce control decisions based on, for example, user identification and/or previous connectivity. At the session level, firewalls can be used to establish a secure and authenticated communications channel regardless of the protocol or application requested.

Firewall implementations and products may be grouped into four major categories, each of which is described below:

1. Stateless packet filters: Also known as screening routers, this category of firewall implementations and products controls traffic at the network (or transport) level by examining source and destination addresses of data packets, source and destination service ports, packet types, and packet options; and either blocking or passing the packet to its intended destination network or network segment. Network access/denial is based on Access Control Lists, which are database files that reside on the firewall, are maintained by the administrator, and tell the firewall specifically which packets can and cannot be forwarded to certain addresses. The firewall can also enable access for only authorized application port or service numbers.

2. Stateful packet filters: Also known as stateful inspection firewalls, this category captures data by an inspection engine operating at the network layer. These packets are queued and then analyzed at all Open Systems Interconnection (OSI) layers by comparing them to a "state table." This table keeps track of inbound and outbound connections and the conversation's state, and discards packets not part of a valid connection in the proper context. The state of the connection is monitored at all times, allowing the actions of the firewall to vary based on the administrator-defined rules and the state of previous conversations. In effect, the firewall is capable of remembering the state of each ongoing conversation across it and dynamically modifying the packet filter rules to suit, thus allowing it to more effectively determine which inbound packets are part of an existing session and which are rogue packets.

   The primary difference between a stateful firewall and a packet filtering firewall is that the packet filtering firewall compares each separate packet to its rule set without regard to any previous packets. The stateful firewall sees each connection as a whole and in context with the normal (layer 3 and 4) behavior of that particular protocol.

3. Application level proxies: Also known as proxy servers, these are programs that reside on a firewall and relay traffic for a specified application, such as Telnet, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), or Hyper Text Transfer Protocol. A proxy server acts as an intermediary for user requests, setting up a connection to the desired resource at the application level. Client applications outside the firewall communicate with the proxy servers instead of directly with application servers. The proxy programs work by transferring a copy of each accepted data packet from one network to another, thereby masking the data's origin. Because they intercept traffic at the application level, they have more insight into the nature of the traffic that they examine. More specifically, a proxy server firewall can

dynamically monitor the behavior of a particular protocol to make sure that the connections are only using the protocol with expected parameters. This can prevent new and unexpected kinds of attacks (or accidental DoS caused by noise from a misconfigured system) without having to wait for software updates to protect against a specific signature. This setup enables an application proxy to control the application communication before allowing the conversation to proceed. Unlike packet filters and stateful inspection firewalls, a direct connection is never allowed between two networks.

Certain kinds of proxy servers can be used to enforce acceptable use policies. An http web proxy, for example, can prohibit user access from certain prohibited sites that either fall outside of acceptable use guidelines, or pose a threat to network security. It can also monitor and log Internet usage for individual systems and users. In the case where a user (either knowingly or unknowingly) downloads malware, or is used in an attack against another system, the web proxy server logs can provide forensic evidence to determine how the security breach occurred, and information on how to prevent such attacks in the future.

4. Circuit level gateways: This category is a variation of application level proxies, providing security for a wide variety of protocols, used when no application specific proxy exists. Like an application level firewall, the circuit level gateway still relays data for a given application back and forth between the internal network and the external network, thus creating a virtual circuit across the gateway. However, the gateway does not perform any control functions at the application protocol level. Instead, it acts at the session or transport level to pass traffic transparently for a given application. A circuit level gateway typically is used as part of a gateway that performs application level proxying and essentially bypasses the control functions of the gateway for a particular application that is deemed not to pose a security threat and for which no application specific proxy exists.

In addition to these main categories of firewalls, in practice, many of today’s commercial firewalls use a combination of these techniques. For example, a product originating as a packet filtering firewall might have since been enhanced with smart filtering at the application level; or application proxies in established areas such as FTP may augment with an inspection based scheme.

While firewalls offer considerable advantages, there are also a number of issues associated with their potential benefit. Many of these advantages and issues are best understood as trade-offs between implementations of the four major firewall classifications; therefore, the determination of the proper firewall architecture is very important to the provision of effective firewall-based security.

Current Strengths

Each category of firewalls has specific strengths. Listed below are strengths of all firewalls and by specific category:

All firewalls:

- Single IP address: Firewalls present a single IP address to the outside world, thus hiding the real structure of a network from intruders.
- Auditing and reporting: Firewalls usually provide full auditing and reporting facilities.
- Inclusion of VPN technology: Many firewalls include Virtual Private Network (VPN) technology, where a secure tunnel is created over the external network via an encrypted connection between the firewalls to access the internal, protected network transparently.
- Ease of configuration for the basics: For users with minimal or basic requirements, firewall appliances of all types provide easy-to-configure integrated hardware and software packages that run on dedicated platforms.
- Difficulty in hacking appliciances: Firewall appliances often have only very elementary OSs, residing on flash (burned on) memory rather than having hard drives and RAM chips. Much of their functionality is hard wired onto the board. Their OSs are usually comprised of proprietary machine level code which is single purpose and therefore not as exposed to the larger hacker world. Appliances tend to be very difficult to hack, with little or no ability to store alien code, such as hacker backdoor programs, without physical access to the device.

Stateless packet filters:

- Cost effectiveness: Packet filter firewalls are generally fast, transparent (no changes required at the client), flexible and cheap. (Most routers will provide packet filtering capabilities; pure packet filters do not require powerful hardware on which to run.)
- Performance: A packet filter firewall usually outperforms an application level firewall because it does less processing of each packet. However, it cannot prevent attacks at the application level.

Stateful packet filters:

- Throughput: Stateful inspection firewalls work well with complex protocols, support new services easily, and work best where security is a concern but throughput is more important. Recently, the technology has achieved phenomenal increases in throughput, and decreases in signal delay through the advent of stateful inspection firewall appliances.

Application level proxies:

- Security: Application level proxies can control the application communication before allowing a conversation to continue (e.g., can require strong authentication), and because there is no direct network connectivity between external networks and the protected server, the protected system is secured from network level attacks (e.g., SYN floods, Ping of Death).

Circuit level gateways:

- Ease of maintenance: Circuit level gateways provide security for a wide variety of protocols and are easier to maintain than application level proxies.

Current Issues

Each category of firewalls has specific issues. Listed below are issues of all firewalls and by specific category:

All firewalls:

- Possible bottlenecks: Few firewalls on the market today provide wire-speed throughput, therefore firewalls have the potential to cause serious bottlenecks, especially for gigabit networks. Careful network design and load balancing across multiple firewall devices is necessary.
- Single security location: A networked-based firewall system concentrates security in one location as opposed to distributing it among systems.
- Insider attack vulnerabilities: Firewalls provide little protection from insider attacks (e.g., insider copying of restricted data). However, VLAN and other network segmentation techniques allow for the use of internal firewalls, most often using router ACLs (packet filtering).
- Back door vulnerabilities: Firewalls do not protect against back doors into the site (e.g., in cases of unrestricted modem access).
- Leakage: Firewalls are subject to "leakage," or accidentally allowing traffic through a filter, and therefore potentially allowing some degree of unauthorized access.
- Lack of protection to underlying OS: A firewall provides little protection to the underlying OS on which it is running. However, the firewall rule set, as well as built-in software access control does provide a measure of protection to the OS of a firewall system and, while it is true the firewall's OS shares the same vulnerabilities as any other system with that OS on the network, it also shares in the protection afforded by the firewall rule set itself.

  A dedicated firewall OS or a hardened general purpose OS may be necessary to provide a secure platform for the firewall. Firewall systems running on UNIX, Linux, BSD or NT can be hardened by disabling all unneeded services in the same manner a bastion system might be hardened. However, there is no guarantee of safety.
- Price performance: There is a very substantial difference in price for performance (or speed) in an appliance-based firewall vs. a firewall application on a traditional OS.

Stateless packet filters:

- Configuration difficulties: Packet filter firewalls are traditionally difficult to configure and provide relatively poor rule verification and logging capabilities.

- Incomplete server protection in some cases: Packet filters will not prevent all network-level attacks against the protected server; several protocols and application services pose problems. These firewalls have limited functionality for protocols which are not connection oriented (like FTP) and are much more vulnerable to certain kinds of attacks that use artificially segmented packets.
- Download and transfer vulnerabilities**:** Firewalls do not protect against users downloading virus-infected PC programs from Internet archives or transferring such programs in attachments to e-mail.
- Cost for required expertise: Packet-filtering firewalls with their limited flexibility and features are relatively inexpensive to purchase (There may already be one built into a router somewhere.) but require advanced expertise which can be costly.

Stateful packet filters:

- Complexity: The core technology of stateful inspection is complex and may have difficulty handling more subtle attacks as they evolve (i.e., it takes time to fully understand the context of the communications).
- Susceptibility to DDoS attacks**:** Stateful firewalls, because of the need to keep state tables, are much more susceptible to DDoS attacks based on techniques like syn floods.
- Greater initial costs: Stateful inspection firewalls have greater initial costs, but allow some on-the-job training with their friendly GUI interfaces, and increased flexibility.

Application level proxies:

- Performance with proxy servers: Proxy servers may impact performance due to large processor and memory requirements for application protocol analysis and support to many simultaneous users.
- Impact to flexibility: Proxy servers may impact flexibility since the introduction of new Internet applications and protocols can often involve significant delays while new proxies are developed specifically to support them.
- Great variance: Proxy firewalls vary greatly in their ease of configuration, features and initial cost.

Ongoing R&D

A primary focus of firewall R&D is on research necessary to understand and enhance the security utility of new firewall-related technologies while also working to identify and mitigate vulnerabilities. Related efforts are as follows: to gain direct experience in the installation, evaluation, configuration, and usage of advanced firewall technologies and architectures; to investigate new technologies for network perimeter defenses, including Asynchronous Transfer Mode; and to investigate the integration of host- and network-based security mechanisms with network perimeter defenses.

A good source for ongoing research can be found at the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) at the following URL on the World Wide Web (WWW, or Web): http://csrc.nist.gov/, and the Purdue University CERIAS homepage located at: http://www.cerias.purdue.edu.

The names and contact information for other current major research centers are shown in a list maintained by Purdue University at the following URL: http://www.cerias.purdue.edu/hotlist/detail.php?arg1=280&arg2=Education+/+Research+Centers

Within this site, the following URL provides the comprehensive list of resources associated with Internet firewalls: http://www.cerias.purdue.edu/hotlist/detail.php?arg1=090&arg2=Network+Security+/+Firewalls

ICSA Labs directs a certification program aimed at testing the security of commercially available firewall products. In their Firewall Lab, security testing is done on a significant number of the firewall products available on the market today. Testing by trained ICSA Labs firewall analysts is conducted against a standard set of functional and assurance criteria elements before receiving the ICSA certification.

Leading Organizations

Leading commercial organizations providing products within the firewall market can be categorized according to the segment of the firewall market they support. The Gartner Group sees the firewall market divided into three primary segments of firewall protection, each best suited functionally for different enterprise objectives. These segments are Enterprise Firewalls, Firewall Appliances, and Embedded Firewalls.

1. Enterprise firewalls**:** This segment consists of software that runs on high-performance workstations on top of Unix or Windows NT OSs. Enterprise firewalls support a wide range of protocols for both outbound and inbound connections, and are the best choice for large enterprises making complex use of the Internet for e-business extranets. Enterprise firewalls can control user access and actions to selected servers, as well as limit downloadable content through Java filters and code signing. Enterprise firewalls need to provide features for managing multiple firewalls from a single management console, both for redundancy and availability and to support distributed firewall architectures.

2. Firewall appliances: This segment runs on proprietary hardware to perform dedicated firewall functions. Firewall appliances, at the low end, do not require extensive OS expertise, thus reducing the amount of support time required to keep the firewall secure. At the low end they generally are appropriate for implementing simple security policies, mostly outbound Internet access and limited protocol support. High-end versions of firewall appliances provide full firewall functionality with integrated VPN capabilities and some loss in flexibility. High and mid-end firewalls, regardless of the platform, do require extensive OS expertise in order to be certain

that the box is properly secured, and to sustain the firewall software or firmware in a stable state.

3. Embedded firewalls: This third segment consists of firewall functionality integrated into a device that also performs other functions, like a PC. Today embedded firewalls consist primarily of personal firewalls, but the technology is rapidly moving toward firewall software on integrated circuits that will be embedded in modems, network interface cards, and motherboards. This will allow firewalls to be embedded in Web servers, Internet appliances, and other applications where software-based firewalls have failed. These firewalls will implement port filtering policies and support VPN connections and central management.

The table below lists some of the leading commercial organizations and products by firewall market segment.

Table 2.4 Leading Commercial Organizations and Firewall Products

Company	Products	Description	Web Site URL
Check Point Software Technologies	Fire Wall-1	Enterprise Firewall	www.checkpoint.com
Symantec Corporation	Symantec Enterprise Firewall (Raptor)	Enterprise Firewall	www.symantec.com
Network Associates	Gauntlet	Enterprise Firewall	www.nai.com
Cisco Systems	PIX	Firewall Appliance-high end	www.cisco.com
Nokia	Check Point FireWall-1	Firewall Appliance-high end	www.nokia.com
WatchGuard Technologies	Firebox II	Firewall Appliance-high end	www.watchguard.com
SonicWall	SonicWall Pro	Firewall Appliance-low end	www.sonicwall.com
WatchGuard Technologies	Firebox SOHO	Firewall Appliance-low end	www.watchguard.com
NetScreen	NetScreen-208, -50, -5XT	Firewall Appliance-low to high end	www.netscreen.com
RapidStream	RapidStream family	Firewall Appliance-low to high end	www.rapidstream.com
Check Point Software Technologies	VPN-1/FireWall-1	Embedded Firewall	www.checkpoint.com
WatchGuard Technologies	Firechip	Embedded Firewall	www.watchguard.com
Secure Computing	Sidewinder	Embedded Firewall	www.sctc.com

Product/Technology Status

Having existed since 1995, the firewall market is relatively mature and stable within the context of the overall Internet products market. In 2000, the firewall market began to move in two directions: toward lower price points for small office, low bandwidth use, and toward higher speed, hardware based platforms for high bandwidth and shared services environments.

Most noteworthy in this trend has been the explosive growth of the firewall/VPN security appliance market. This market is defined as the combination of hardware, software, and networking technologies whose primary function is to act as a firewall and to come equipped with VPN capabilities. By 2000, this market more than doubled in size from 1999, with total revenue over $900 million. By 2005, it is estimated that the market will grow to $4 billion [5]. For comparison purposes, the software firewall market in 2000 had a total revenue of about $700 million and is expected to reach $1.5 billion by 2005 [6]. The firewall software market consists of software that identifies and blocks access to certain applications and data. Firewall software can function as enterprise or embedded firewalls.

Firewalls are a mainstay of any security program where Internet access is involved. There are numerous firewall vendors of all sizes worldwide, supplying products to each of the firewall sub-markets. However, most of the market share is concentrated in a handful of market leaders.

Check Point Software Technologies is the entrenched enterprise firewall leader. It is the product of choice for global enterprises with multiple Internet gateways and VPN requirements. Checkpoint is pressured from below by firewall appliance vendors that offer simpler set-up and management options, as well as lower costs. Pressure from above is being exerted by Cisco Systems with its high throughput firewall appliances in the gigabit wire speed range.

Also in a leadership position, Symantec is the only market leader with a powerful suite of security management tools. With the increasing need and importance of this capability, Symantec has the opportunity to leverage management and reporting, as well as integration with other security devices in the competition for enterprise sales.

Technology Selection Considerations

1. Criteria that could be used to evaluate and compare firewall technologies:

    - Extent to which a firewall must support and enforce a usage (e.g., Internet) policy
    - Adherence to an existing agency standard that details the specific firewall that should be acquired
    - Existence of a certification or warranty by the vendor to perform in an acceptable manner

- Traffic volume and connectivity requirements that the firewall must support
- Specific hardware and software required by the firewall
- System administrative skills required to support the firewall and what vendor support is available
- Cost of firewall

2. Current performance considerations:

- Firewalls can range from host based personal firewalls serving a single user and a simple security policy to networked based enterprise firewalls serving large organizations with complex security policies.
- The costs can range from around one hundred dollars to over ten thousand dollars.
- Packet filtering firewalls tend to be faster than application-level firewalls and consequently tend to have greater throughput and lower latency.
- Firewall appliances, at the low end, do not require extensive OS expertise, thus reducing the amount of support time required to keep the firewall secure, whereas high end enterprise firewalls tend to be quite complex, requiring extensive OS and maintenance expertise.

3. Evaluation and testing considerations:

- The relative maturity of firewalls as an ISS technology lends itself to the use of established testing and certification organizations as part of the firewall selection process.
- For instance, ICSA Labs, http://www.trusecure.com, directs a certification program aimed at testing the security of commercially available firewall products. In their Firewall Lab, security testing is done on a significant number of the firewall products available on the market today. Testing by trained ICSA Labs firewall analysts is conducted against a standard set of functional and assurance criteria elements before receiving the ICSA certification.
- Another such organization is the Computer Security Institute (CSI). CSI maintains the "CSI Firewall Product Search Center," www.spirit.com/CSI/firewalls.html. The Firewall Product Selector that can be accessed from this site allows you to specify desired characteristics for your firewall. A ranked listing of firewall products is provided, based on closeness of fit between your requirements and their firewall database. At this point you can request a detailed description of any of the selected firewalls, or obtain a detailed comparison of two or more firewalls on the ranked list.

Technology Insertion

Firewalls are being used currently in the FAA. The FAA should follow the development of this now established technology, and upgrade and integrate firewalls to match future requirements.

Future of Firewalls

A significant trend in firewalls is the increased integration of firewalls with other parts of the network infrastructure. This is indicated by the addition of new functionality (high availability dual systems, network management, applet monitoring, virus scanning, network protocol hardening, and encryption) and the overlap of firewalls with other security measures.

For example, internetworking products have been developed with built in firewall protection capabilities such as stateful inspection and encrypted tunneling for VPNs. Also, some firewall products now include support for next generation IPs such as IPv6 that include more security at the network layer.

In the near future, the following forecast can be expected:

- Firewall functionality will continue to be incorporated into the network infrastructure as networking devices gain more powerful firewall features and become more trustworthy.
- Firewall features will be embedded in OSs, thereby easing interoperability problems.
- There will be increasing need to manage multiple firewalls by enterprises supporting multiple Internet connections.
- There will be rapid growth in the managed firewall services market, as organizations require better firewall management, data analysis and reporting capability.
- There will continue to be growth in the market for hardware-based firewall appliances that sacrifice flexibility in favor of easy configurability, but retain similar functionality to firewalls running on general purpose platforms.
- The number of firewall appliances providing gigabit speed capability will increase, as vendors provide faster firewall/VPN security appliances to meet the needs of large enterprises and service provider customers demanding high speed connections.
- There is a market emerging for "in-the-cloud" firewalls that operate at high speed (1-10 Gbps) and allow managed firewall service providers to eliminate the need for customer premise equipment.
- Real time intrusion detection will grow as a means of validating the firewall, allowing network administrators to detect break-ins as they occur.

2.2.2 Intrusion Detection Systems (IDSs)

As network attacks have increased in number and severity over the past few years, IDSs have become a necessary addition to the security infrastructure of most organizations. Intrusions are defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusions are caused by attackers accessing the systems from an external access point, such as the

Internet, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given them.

IDSs are software and hardware devices that automate the process of monitoring the events occurring in a computer system or network, and analyze them for signs of security problems. Typical IDSs have three functional components: information sources, analysis, and response. IDSs obtain event information from one or more information sources, perform a pre-configured or heuristic-generated analysis of the event data, and then generate specified responses, ranging from reports to active intervention, when intrusions are detected. The primary issues that motivate IDS product choices and architecture are:

- System monitoring approaches: Most IDS products specialize in network-based, host-based, or applications-based monitoring.
- Analysis strategy: Most IDS products use pattern matching and system change detection to identify attacks, while some use anomaly detection or a hybrid of the two.
- The timing of information source and analysis: Most IDS products are designed to provide alarms on-demand, interval-based, or real-time. Response time requirements, as well as staffing decisions, should be used to determine which product is most applicable.

IDSs are commonly used in combination with vulnerability analysis and firewalls. Each security protection service addresses a particular kind of security thread. Only by combining them (i.e., defense in depth) can the system be protected from a realistic range of security attacks.

Vulnerability analysis systems are very similar to IDSs, as they both look for specific symptoms of intrusions and other security policy violations. However, vulnerability analysis systems take a static view of such symptoms, whereas IDSs look at them dynamically. This is similar to the difference between taking a snapshot of an incident versus videotaping it.

Firewalls serve as barrier mechanisms, barring entry to some network traffic and allowing others, based on a firewall policy. IDSs serve as monitoring mechanisms, watching activities, and making decisions about whether the observed events are suspicious. They can spot attackers circumventing firewall and report them to system administrators, who can take steps to prevent damage.

Current Strengths

- Product choices: There are many commercial IDSs available in the market place, each of which is designed for different requirements and goals of an organization.

- Dynamic analysis: IDSs can evaluate system events dynamically and take appropriate action to minimize system damage.
- Monitoring support: While they have many limitations, IDSs can provide quality support for monitoring system activities and for the system administrators by identifying suspicious events and taking actions as designed for the specific IDS.

Current Issues

IDSs have many limitations. These are the major ones:

- Scalability: Many commercial IDSs are not scalable to large or distributed enterprise networks.
- Management: IDSs can be difficult to manage, with awkward user control.
- Analysis capabilities: Commercial IDSs rarely contain effective user analysis systems for viewing alarms and making effective decisions. It is often easy for a human analyst to be overwhelmed with alarms. Additionally, many IDSs conceal their rule sets or do not document them, making it difficult to determine exactly what was caught.
- IDS interoperability: Different commercial IDSs rarely interoperate with each other.
- External interoperability: Commercial IDSs rarely interoperate with other security or network management packages.
- Error rates: There are significant error rates in IDS results, especially for false positives, but also for false negatives. Additionally, many attackers launch attacks without regard to whether the target is vulnerable (e.g., IIS web server attacks launched against Solaris web servers), which will set off alarms despite a lack of effective intrusion.
- Organizational hurdles: An IDS cannot compensate for significant deficiencies in an organization's security strategy, policy, or security architecture. Additionally, effective incident response will be impossible without accurate inventory management and management support.
- Visibility: In order to function properly, network-based intrusion detection systems must be placed in network locations that have the strong potential of seeing malicious network traffic. The increasing use of network switches and cryptography can inhibit the ability of an IDS sensor to view malicious network traffic. Effective IDS deployment requires a good understanding of the relevant organization's network topology.
- Latency: Logging activities from IDSs can impose significant network performance degradation if care is not taken in building the network architecture. IDSs often require that switches and routers be configured to provide mirror ports, which can severely impact performance of normal network operation.

- False Expectations:
  - IDSs cannot compensate for security weaknesses in network protocols.
  - IDSs cannot substitute for other types of security mechanisms (e.g., identification, authentication, encryption, or access control).
  - IDSs do not protect a system from security threats; rather, they detect intrusions only after they occur.

Ongoing R&D

While the IDS research is maturing, various systems that log unsuccessful access attempts have been in use since the 1970s. Some commercial IDSs have received negative publicity due to large number of false alarms, awkward control and reporting interfaces, overwhelming numbers of attack reports, lack of scalability, and lack of integration with enterprise network management systems.

There are trends in computing that will affect the form and function of IDS. It is also likely that certain IDS pattern-matching capabilities will move to hardware in order to increase bandwidth. Below are a number of research activities in the area of standardization and interoperability:

- Audit trail format
- Universal format for logger messages
- Intrusion detection working group
- Common intrusion detection framework
- Common vulnerability and exposures.

Leading Organizations

The following tables list research activities/technologies, the leading companies or institutes, and contact information that are working on these projects, technologies, and standards.

Table 2.5 Leading Organizations

Research Activity/Technology	Company/Institute
Audit trail format	University of Purdue
Universal format for logger messages	Internet Engineering Task Force (IETF)
Intrusion detection working group	IETF
Common intrusion detection framework	ISI
Common vulnerabilities and exposures	MITRE

Table 2.6 Points of Contact

Research Activity/Technology	Website/Contact
Audit trail format	http://www.cerias.purdue.edu/coast/projects/audit-trails-format.html
Universal format for logger messages	http://www.didc.lbl.gov/NetLogger/ulm_format.html
Intrusion detection working group	http://www.ietf.org/html.charters/idwg-charter.html http://www.semper.org/idwg-public/idwg-public-request@semper.org
Common intrusion detection framework	Dan Schnackenberg: dan@baker.ds.boeing.com Brian Tung: brian@isi.edu http://www.isi.edu/gost/cidf
Common vulnerabilities and exposures	http://cve.mitre.org

Table 2.7 Current IDS Products

Product	Operating Systems		Deployment Strategy		Information Source							Method		Real-time Processing		Initial Release
	NT	UNIX-based	net-based	host-based	network packets	OS	Web server	router	firewall	file system	other	know-ledge	behavior	yes	no	year
1. Symantec Intruder Alert (ITA)	X	X		X		X	X			X		X		X		1992
2. Symantec NetProwler	X		X		X							X		X		1997
3. CISCO Secure IDS		X	X		X							X		X		1996
4. ISS RealSecure	X	X	X	X	X							X		X		1996
5. Intrusion.com SecureNet PRO		X	X		X							X		X		1997
6. Tripwire	X	X		X						X		X			X	1998

THIS PAGE LEFT INTENTIONALLY BLANK

Product/Technology Status

The current trends in internetworking are likely to present serious challenges to the way in which IDSs currently operate. VPN technology relies on the ability to encapsulate packets inside the payload of other packets, and encryption technology makes it virtually impossible to peer into the contents of most of this payload and look for attack signatures.

In addition, network gateways have become increasingly reliant on near-wire-speed switching at higher protocol layers, making packet forwarding decisions based on select portions of the packet header. Intrusion detection is likely to become a larger bottleneck as switch speeds move into the multigigabit per second range, and vendors find themselves no longer able to offer a promiscuous port option without sacrificing the performance of their switching equipment. One possible solution to this problem is to implement distributed IDSs featuring several collectors that share a high-performance database backend, which can then aggregate the data in near real time.

Deploying an effective IDS is a challenge, but much more significant is the commitment of time and effort necessary to ensure that an enterprise maximizes the benefit from the system, including the inherent research and the constant updates of intrusion alert rules. The security administrator has a major responsibility in maintaining the most current and effective IDS configuration.

Technology Selection Considerations

1. Criteria that could be used to evaluate and compare IDS technologies:

    - Accuracy: Type I, type II error rates from user trials or published product reviews
    - Ease of use: User ratings from user trials or published product reviews
    - Downtime: Hours/minutes/days from user trials or published product reviews
    - Cost

2. Current performance considerations [7]:

    - Should be able to reliably identify the most common attacks: SYN flood, Code Red worm, wu-ftpd exploit
    - Should be able to be configured so as to reliably identify and report on traffic intrusions without halts, crashes and reboots
    - Should be able to be operational 99% of the time or better
    - Cost range: $12.5-$25K; product should provide superior performance to open source “freeware” alternatives

3. Evaluation and testing considerations:

    - The evaluator needs to fully understand the terminology involved with IDSs in order to read product descriptions, talk with vendors, and evaluate IDS products.
    - The evaluator should seek the most up-to-date product reviews for guidance.

- As the current IDS products are immature, the evaluator should demand a minimum of a 30-day trial prior to purchase, as well as vendor assistance in configuration and training.

Technology Insertion

IDSs should be a part of the FAA security architecture, but, again, they should not be viewed as a single technology solution, but should be used with other ISS technologies in a multi-layer strategy. There are a variety of IDSs on the market that could be inserted into the FAA environment today. These IDSs have considerably different capabilities and support provisions, so the FAA must look closely to ensure a match to requirements.

Future of IDSs

A recent trend that is expected to accelerate in the future is the sharing of intrusion information and the formation of central incident response centers, such as the Federal Computer Incident Response Center (FedCIRC), www.fedcirc.gov, and the FBI's National Infrastructure Protection Center, www.nipc.gov.

An industry example is the recently formed Internet Storm Center, sponsored by the SANS Institute, which has been effective in discovering new worms as they are launched. It is like the weather service where sensors (more than 2,000 in 45 countries) feed data to analysis centers. Computers with Zone Alarm, McAfee, PIX, IPChains, Snort, and several other systems all send intrusion and log data that provide a real-time map of attacks on the Internet. These data can be seen in real-time at www.incidents.org or www.dshield.org, and www.mynetwatchman.com. One of the best features is that they aggregate attack data and respond by pushing Internet Service Providers (ISPs) to inform people whose machines are being used in attacks.

2.2.3 Malicious Code and Virus Detection Systems

Nearly all computer systems are susceptible to viruses, Trojans, and worms if they are connected to the Internet, use removable electronic media, allow unsupervised access to users, or use shareware. Viruses, Trojans, and worms are all different types of malicious code that are sometimes referred to collectively as "viruses," even though each type operates differently. The distinguishing feature between types of viruses is its method of propagation (e.g., self-replication, user action, and host-based replication).

A computer virus is a string of code developed for malicious purposes that attaches itself to another computer program or document. Once it is attached, it replicates itself by using some of the resources of the co-opted program or document to replicate and attach itself to other host programs and documents. There are three categories of viruses: file infectors, boot-sector viruses, and macro viruses.

Malicious code is not limited to viruses, but several other types of malicious code are generally detected by anti-virus (AV) software. These other categories of malicious code include the following:

- Worms: This category of malicious code is particular to networked computers. Worms are self-replicating programs (unlike viruses which need a host program to replicate) that work their way through a computer network exploiting vulnerable hosts and causing whatever harm they were programmed to accomplish.
- Trojan horses (or Trojans): This category is designed to fool a user into thinking that it is benign. A Trojan is a program placed on a system by a hacker or installed unknowingly by the user that conducts malicious actions while hiding or pretending to do something useful.
- Malicious Mobile Code: This category is a relatively recent development that has grown with the increased use of Web browsers. Mobile code is used by many Web sites to add legitimate functionality and includes ActiveX, JavaScript, and Java programs. Unfortunately, mobile code has vulnerabilities that allow the creation of malicious programs. A user can infect a computer with malicious mobile code just by visiting a web site.
- Spyware: This category of malicious code is used to systematically collect information from sensitive government or business entities. Various active agent web applets can be covertly installed on enterprise networks to provide a complete picture of its administrative and operational systems.

AV software scans a computer's memory and disk drives for viruses. If an AV scanner finds a virus, the application informs the user and may clean, delete, or quarantine any files, directories, or disks affected by the malicious code.

There are two fundamental types of AV products: signature-based AV scanners and behavior-based (or policy-based) middle ware.

- Signature-based anti-virus applications: Signature-based AV products are response systems that can regularly download updated virus signature files from the vendor. New signatures are continually being generated as new viruses (or their variants) are released on computer systems. A virus signature is a search pattern, often a simple string of characters or bytes, expected to be found in every instance of a particular virus. Usually, different viruses have different signatures. Anti-virus scanners use signatures to locate specific viruses. In today’s network environment, signature files are regularly and automatically updated (e.g., every week).

  Many AV-signature scanners are available to detect viruses, Trojans, and worms contained in e-mail, floppies, CD-ROMs, hard-disks, and documents. Certain AV scanners also detect malicious code from web sites. No matter what type of AV scanner is being used, it cannot offer its full protection unless it has an up-to-date virus signature database. To detect viruses, the AV scanner compares file contents with known computer virus signatures, identifies infected files, and repairs them (if possible) or quarantines them (i.e., blocks access to them) if not possible to repair. More sophisticated programs also look for virus-like activity in an attempt to identify new viruses or variants.

- Behavior-based anti-virus protection: A behavior-based (or policy-based) AV system prevents malicious applications or user actions from manipulating the system resources if the actions do not comply with system policies. This technique can only be used when the virus is active. It prevents the malicious behavior of the virus once it is within the network environment.

  To complement AV scanners, several behavior-based AV protection systems have been developed. These behavior-based models are rapidly growing in acceptance among enterprises. Behavior-based protection provides protection against polymorphic viruses, self-replicating applets, network-borne attacks, internal saboteurs, and uninformed users. Behavior-based AV protection offers many advantages over an AV signature scanner:

  – Does not require continuous updates.
  – Prevents potentially damaging behavior by monitoring the code as it executes.
  – Monitors and enforces network policies.
  – Covers an enterprise during its most vulnerable time -- before the signature file is updated.

  Behavior-based models use one of several techniques: trusted content, executable wrappers, and policy enforcement middleware, which are described in the following sub-sections:

  – Trusted Content: Viruses can be thwarted by locking down all PCs to only allow trusted software (i.e., executables) to be executed. This approach greatly limits PC users' flexibility and places a large maintenance burden on the IS organization.

    Another approach is to require all executables to be digitally signed, and to configure PCs to check digital signatures on programs before execution. The software will be allowed to run only if the code has been signed by a trusted authority. There are several major weaknesses in relying on code signing. The IS organization will be required to test and sign every executable before it can run on a corporate PC, which means that this approach is not much different than simply locking down all PCs. If the IS organization decides to trust software signed by a trusted vendor, it will trust all software signed with that same signing key, which leads to its own set of vulnerabilities.

  – Executable Wrappers: Executable wrappers check incoming executables against a set of electronically stored policy controls, effectively limiting the actions an executable can take. This approach implements policy controls around the application. The downside is that the wrappers must be applied before the suspicious executable reaches the PC, which works fine when PCs are behind the corporate firewall, but leaves vulnerable those laptops that connect remotely.

– Policy Enforcement Middleware: Implementing security middleware between the operating system and all executables can be a very effective technique to enforce policy-based controls, which define what actions an application is allowed to take. The middleware intercepts all calls to the OS and blocks actions that violate defined policy. These controls can be specific to known applications, such as not allowing an application to e-mail itself to everyone in the address book, or can be more generic for customer software, such as not allowing any application to delete the contents of the hard drive or replace another executable.

The following is a list of behavior-based AV products (middleware) available for enterprise-level AV protection:

- InDefense's Achilles' Shield, (www.indefense.com): This is behavioral-based protection to defend against file infecting viruses, boot sector infectors, system registry modifications, and to defend Microsoft® Outlook mail, and Microsoft® Office files, including Word™, Excel™, Access™, and PowerPoint™ files. InDefense technology is based onmultiple layers of protection, each designed as a barrier to areas of the system commonly targeted by malicious programs.
- Aladdin Knowledge Systems' eSafe, (www.ealaddin.com): This product detects viruses in encrypted e-mail that only reveal themselves when the e-mail is run. The control option of eSafe uses SurfControl for content filtering, which blocks dozens of categories of URLs. Offensive word lists come in a multi-language compilation. Subscriptions provide automatic updates for all services.
- Pelican Security's SafeTnet, (www.pelicansecurity.com): SafeTnet blocks the intruder at the entrance to the computer and monitors each step the code attempts, recognizing any action that does not match the predetermined safety requirements. This approach is taken instead of "blacklisting" known dangers, leaving critical corporate assets, data, applications, network and system files vulnerable to unknown attacks and to compressed, encrypted or changed code which are unrecognizable to regular AV programs.
- Finjan's SurfinShield Corporate, (www.finjan.com): SurfinShield is a centrally-managed enterprise PC solution that monitors the behavior of programs in its "Sandbox." SurfinShield's Sandbox enforces security policies to automatically block malicious activity before damage can be inflicted. Examples of security policy violations include attempts to delete files, open network connections or access the system registry.
- Entercept Security Technologies, (www.entercept.com): Entercept is a multi-layered server security solution. It identifies and stops known and unknown intrusions that exploit services (such as Web, Mail, DNS, FTP, etc.) before malicious code is executed. Using an extensive intrusion dictionary and an exclusive behavior model, Entercept can identify and stop generic and specific intrusions.

Current Strengths

- Complementary: Both signature-based AV scanners and behavior-based AV products complement each other. AV signature scanners are reactive, whereas the behavior-based products are proactive. In addition, AV protection software is further delineated between desktop applications and server (e.g., e-mail server) applications. Again, both types of products complement each other. In today's networked environment, both desktop and server AV applications should be utilized for a combined approach to virus protection.
- Proactive prevention: The primary strength of behavior-based AV protection is that it proactively prevents damage from malicious code, human error, and other behaviors, whether they originate from internal or external sources. It allows one to go into the operating-system kernel and set up rules that prevent strange behavior on the system. Since behavior-based models protect at the kernel level, it will cover the signature-to-download gap.
- Runtime monitoring: These tools define potentially dangerous actions that should be monitored at runtime (e.g., modifying Windows registry, write access to specific files or directories) and intercept code that tries to do them. The user/system administrator can create security profiles/policies that the runtime monitor implements.
- Reduced costs at the enterprise level: The costs and security risks of maintaining updated AV signatures can be reduced substantially by using centralized enterprise-wide AV administration to distribute updates.

Current Issues

In 2001, new viruses were detected on the average of every 18 seconds. Keeping signature files up-to-date is by necessity a continuous process. Signature-based AV products can only stop viruses or worms that have known signatures. Unknown signatures require a patch, which is often not available for a number of days.

- Time gaps for virus signatures: The primary issue of signature-based AV protection is the lag time between virus generation and virus protection. The speed at which viruses spread is faster than the speed to develop and distribute virus signatures for AV protection. There are two gaps in time of signature-based AV scanners:
  - Gap 1: The gap between when a new virus is released and when the AV vendor creates a new signature.
  - Gap 2: The gap between when the new signature is created and when enterprises receive signature files and implement the update at every desktop.

  The AV vendors have done a good job at getting Gap 1 down to a matter of hours. At the desktop, Gap 2 is still measured in days, if not weeks. As employees increasingly use laptop computers that are often only sporadically connected to the corporate network, this gap increases significantly.

Given the trends in the number of viruses, desktop virus signature-based AV protection will become increasingly less effective over time. The gap between the creation of the larger number of new signatures and the time needed to update each desktop will never be close enough to allow signature-based AV software to be completely effective.

- Increasing cost: The cost of maintaining current AV solutions has risen exponentially for the enterprise since 2000, primarily due to increased update requirements. Enterprises now receive signature updates from AV vendors on a daily or weekly basis. Updating once or twice a month was considered best practice only 18 months ago. It is estimated that during a major new virus outbreak, fewer than 20 percent of enterprises manage to update all desktop AV signatures before a virus runs its natural course.
- Web-based services: Since the vast majority of viruses are spread via e-mail, AV solutions at the e-mail server are the most effective in stopping or minimizing the spread of most viruses to the desktop. However, the rise of Web-based e-mail services (e.g., Hotmail, Yahoomail, AOLmail) has opened an e-mail virus path around the enterprise mail AV protection.

  While today's viruses mainly use attached executables as the malicious payload, active content and the coming wave of Web services will present further virus problems for enterprises. These types of software will be more difficult to simply block at the firewall, as evolving online business process integration will require their use. The rise of peer-to-peer communication services also greatly increases the variety of executables that can be sent directly to PCs.
- Mobile Devices: The explosive growth of wireless devices in the corporate environment that are able to transmit, store, and receive data is a growing concern to corporate IT departments. The mobile Internet shares all the potential security issues and risks of the wired Internet as well as the additional risks caused by mobility and the broadcast nature of wireless transmissions. Corporate employees are increasingly creating, accessing, storing, and processing company information via mobile devices, creating an urgent need for security solutions that consistently provide protection.

Ongoing Research

- Florida Institute of Technology: Dr. James A. Whittaker,[1] Director of the Center for Software Engineering Research, CS Dept at Florida Institute of Technology[2] is conducting research under Office of Naval Research funding on behavior-based (policy-based) AV models. This research is a collaborative project with the Computer Science departments at University of Tennessee and University of Central Florida. Dr. Whittaker has co-authored a paper entitled: "Proactive, Selective

[1] E-mail: jw@cs.fit.edu; phone: 321-674-7638.

[2] http://www.cs.fit.edu

Behavior Filtering with Data Restoration: New Technique for Runtime Neutralization of Malicious Mobile Code."[3]

- European Institute for Computer Anti-Virus Research (EICAR): EICAR is a research organization whose objectives are to unite efforts against writing and proliferation of malicious code, such as computer viruses or Trojan Horses; and to develop solutions to prevent computer crime, fraud, and the misuse of computers or networks; and malicious exploitation of personnel data. This organization includes participants from universities, industry, privacy protection organizations, and media plus technical, security and legal experts from civil and military government and law enforcement. Currently EICAR has the following task forces:

  – Task force on cyber defense alliance
  – Task force on critical infrastructure protection
  – Working Group 2 on anti-virus practices
  – Task force on European cyber crime initiative

  Task force activity reports are published either in the regular EICAR "news," or are sent on request directly to members, or are published on their web site: http://www.eicar.org

- IBM AV Research: IBM AV Research provides assistance in the development of IBM commercial-grade AV solutions. The IBM AV research group documents its findings and provides relevant scientific papers on its web site. Currently one question being investigated is whether cryptography can be used to prevent computer viruses. The web site is: http://www.research.ibm.com/antivirus/SciPapers.htm.

- International Computer Security Association (ICSA): Established in 1989 as an independent corporation, the ICSA has successfully led the security industry in the development of high quality security products through product certification programs and in establishing better security practices through management of multiple security-focused consortia. The ICSA web site is: http://www.icsa.net.

Leading Organizations

Leading organizations in AV protection applications are:

- Network Associates (*McAfee Total Virus Defense*) - http://www.mcafee.com

- Symantec (*Norton AntiVirus*) - http://www.symantec.com/nav/

- Computer Associates *(eTrust Antivirus, eTrust InoculateIT, eTrust EZ Antivirus*) - http://www.ca.com/products

[3] To download complete description of project, go to the FIT URL: http://se.fit.edu/projects/

- Trend Micro (*InterScan)* - http://www.trend.com/
- F-Secure (F-*Secure Anti-Virus*) - http://www.F-Secure.com/
- Sophos (*Sophos Anti-Virus*) - http://www.sophos.com/
- Finjan (*SurfinGate*, *SurfinShield*) - www.finjan.com
- Sybari (*Antigen*) - http://www.sybari.com

The top four vendors in the AV market are Symantec, Network Associates, Computer Associates, Trend Micro.

The following behavior-based AV applications are commercially available for enterprise-level AV protection:

- InDefense's Achilles' Shield (www.indefense.com);
- Aladdin Knowledge Systems' eSafe (www.ealaddin.com)
- Pelican Security's SafeTnet (www.pelicansecurity.com)
- Finjan's SurfinShield (www.finjan.com)
- Entercept Security Technologies (http://www.entercept.com)

Product/Technology Status

There exists no single security solution against viruses in mobile devices. The impact of a virus designed for mobile devices may well become more devastating and hence more attractive for a computer criminal. To defend mobile devices against viruses is to secure the entire enterprise.

Behavior-blockers and access-control applications have an advantage over conventional AV scanners in that they do not need to know anything about a virus, worm, or other malicious software in order to work. They are also not fazed by compressed or encrypted code. Most important, these programs are able to deal with Java and ActiveX threats, which are usually totally ignored by virus scanners.

The downside of behavior blockers is that most act like perimeter alarms, popping up dialogue boxes that prompt users to make a choice between stopping or allowing a suspicious action. These warnings often impede productivity, cause application errors or lock up systems. These problems will often prompt a relaxation in security policies, which obviously diminishes the effectiveness of the behavior blockers.

Technology Selection Considerations

1. Criteria that could be used to evaluate and compare AV technologies:

    - Cost
        - for desktop product
        - server-level, network-based product
    - Compatibility with multiple operating systems
    - Type of anti-virus protection needed
        - Signature-based
        - Policy-based (behavior-based) products
        - Integrated product doing both signature-based and policy-based detection
    - Recovery mechanisms
        - Does the product do more than detect a virus?
        - Does it also try to eradicate the problem?
    - Ease of implementation and maintenance (GUI, automated features)
    - Analysis and reporting capabilities

2. Current performance considerations:

    - Cost for PC signature-based antivirus products range from $30 - $80 per machine.
    - Network level and/or policy-based solutions is variable and dependent on many factors and requirements.
    - Integrated solutions that detect malicious code at the desktop as well as at the network level are essential for maintaining the health of the enterprise information systems. Product suites should include both static (signature-based) and adaptive (policy-based) functionality.

3. Evaluation and testing considerations:

    - The *International Computer Security Association* (*ICSA*) has been performing tests of antivirus software since 1992. ICSA Labs, a division of TruSecure Corporation, and West Coast Publishing's *Secure Computing* are commercial testers with various for-fee certifications to antivirus product developers. As most of the top products are certified, to some degree, by both ICSA and *Secure Computing*, while these certifications provide a good base-line, they are not entirely helpful in differentiating between products from the standpoint of virus detection.

    - Ideally, a person or group should be assigned to ensure that the corporate antivirus software is up to the task. This office should use the work of the other testers that have been outlined, as well as to make use of a tool to test the other, non-virus-related properties of the product –the European Institute for Computer Anti-Virus Research (EICAR) test file (available from http://www.eicar.org).

Technology Insertion

Currently available AV tools are used now at the FAA, recognizing that the updates for signature-based tools must be performed and managed faithfully in order to receive the benefit of the tools. The FAA should monitor the progress of the behavior-based solutions and consider moving to that technology after 2005, if those solutions prove to be more effective.

Future of AV Software

Malicious-code detection and handling tools will change from predominantly signature-based solutions to predominantly behavioral-based solutions by 2005, partly due to the growth of Web services and increasingly active malicious software. Major vendors in the AV market have been shifting their focus beyond the desktop by doing the following:

- Expanding their businesses into secure content management
- Moving from product-based models to subscription models
- Expanding into the mobile and wireless markets
- Shifting their AV product focus to servers and gateways
- Using behavior-based (i.e., policy-based) virus detection and prevention.

As network-based firewall, IDS, and other bandwidth-related security services emerge through 2002 and 2003, policy enforcement middleware AV protection will become essential. AV protection in the near- to mid-term should include a variety of malicious-code approaches and policy enforcement.

Heavy desktop-client approaches to malicious-code management are contrary to the "anywhere, anytime" access to data that Web services are based on. Behavior-based policy enforcement will be resisted by vendors of Web services offerings. In addition, OS and office suite vendors have shown they are unable to build robust malicious-executable protection into their products. Therefore, add-on AV software will be required for all desktops through 2005.

- Servers and Gateways: Corporate environments are migrating to server-based and gateway AV implementations because the majority of viruses are now delivered via the Internet (network and mail based). Viruses increasingly seek to either disrupt or destroy the functionality of corporate mail systems. However, protection at the desktop remains important, especially considering the growing number of handheld devices that are linked to corporate PCs on a daily basis that could transmit a virus to the corporate network.
- "Smart" Virus Prevention: Customers have increasingly asked for better virus detection techniques following the worldwide damage that the Love Bug virus caused to corporate e-mail systems. A number of vendors are working on smart AV

technologies, which they believe will be able to stop new (unknown) viruses before they can enter the corporate network. These new smart AV technologies keep executable programs contained in e-mail messages quarantined until the software can determine what the executable program will do. If the executable attempts to do something that the corporate network administrator has deemed unauthorized, the file (and sometimes the entire message) can be blocked until it can be inspected.

2.2.4 Mobile Code Defense

Mobile code is code that is sourced from a remote, and possibly untrusted, system but executed locally. Other names for mobile code are mobile agents, downloadable code, executable content, active capsules, and remote code.

The increase in distributed computer and telecommunication systems has increased the demand and needed support for mobile code. The best known examples of mobile code are applets downloaded from the Internet, but also dynamic e-mail and Telecommunications Information Networking Architecture building blocks.

The concept of using code from possible untrustworthy sources has been in use for many years. Many people have used freeware and shareware over time even though they knew there were risks associated with using software whose internal construction, accuracy, and general trustworthiness were not known. These exchanges of code have provided fast solutions to certain problems, but the code in these exchanges has sometimes also brought a variety of problems.

The tradeoff for using mobile code is providing users of IT systems with the ability to execute software of unknown, or possibly hostile, origin without putting sensitive information and resources at risk of disclosure, modification, or destruction. Mobile code is intended for quick, lightweight execution, such as with applets. The small size and the increasing number of the mobile code units present a problem for the system mechanisms that are designed for, and whose overhead is more relative to, larger applications.

Technically, there three main approaches to mobile code defense [8,9]. The first, “firewalling” or code inspection, examines the executables (the “signatures”) as they enter a trusted domain and decides whether to allow them to run on the client on the basis of their properties. Most believe that this approach, though straightforward to implement, is fundamentally limited by the “halting problem.” (The “halting problem” is the axiom that states that no general-purpose algorithm can determine the behavior of an arbitrary program.) A second approach, variously known as the “sandbox” model, “behavioral controls” or “dynamic monitors,” limits the privileges of the mobile executables to a small set of operations. The difficulty with the sandbox approach lies in administering the attendant security manager, where an error in a security component can lead to violations. A third approach, code signing, would seem to meet the security problem head-on by requiring that clients only use “signed” mobile executables they trust. This technology, used in Microsoft’s Authenticode system for ActiveX, has its own set of weakness, as its binary approach to security leaves the client completely unprotected once penetrated.

The Role of Policy

A key factor in managing the mobile code issue is development of strong security policy that determines what type access any mobile code unit has. Being able to tell in advance whether a mobile code unit will attempt to do harm or not is a difficult if not unsolvable problem today. In view of that, organizations must develop strong security policies to protect the IT resources that could be damaged by malicious mobile code. The DoD has developed a mobile code policy which can be used as an example:

http://www.c3i.osd.mil/org/cio/doc/mobile-code11-7-00.html

Practical mobile code policy requires dealing with a growing number of potentially malevolent technologies: cookies, Java applets, ActiveX executables, rogue servers that dispense "pseudo cookies," and snoop (or spy) ware. As one prescient commentator observed, many security administrators are unaware of the ubiquitous nature of these programs, and although they do not present the greatest security risk today, they are among the most difficult to contain and control.

A full-scale treatment is beyond the scope of this document; the growing literature on mobile code defense is referenced [10, 11, 12, 13]. Two aspects of mobile code policy will be discussed here: cookies, the most ubiquitous, and snoop (or spy) ware, the most immediately troubling from a computer security perspective.

Cookies are a clever programming trick devised by the Netscape developers to create transaction persistence in the otherwise stateless HTTP world. By issuing cookies it allows persistent, customized sessions -- enabling the e-commerce shipping cart. Physically it is accomplished by the web commerce server depositing up to 20 strings of 4,096 bytes each on the client's hard disk.

From a security perspective, this "web guano" has been characterized as a "mistake carried through to perfection." The properties of cookies open a huge number of potential security doors:

- The data is binary encoded or encrypted and difficult for the casual observer to understand;
- The content of the cookies is determined exclusively by the server;
- Cookies can record information about the clickstream of the web surfer;
- Cookies can be shared by third-party hosts with neither the user's knowledge or permission ("third party cookies");
- Cookies can be invoked by servers to produce denial-of-service attacks ("cookie storms");

- Web browsers may store cookies from unvisited sites without the user's knowledge;
- Browsers do not allow cancellation of cookies accepted prior to disabling cookies on one's browser; "tossing your cookies" must be accomplished manually; and
- Cookies are stored in a variety of places on one's hard drive, and with Netscape and Microsoft handling cookies in different ways, their management is made even more difficult.

Thus far cookie abuse has been limited to hijacking web sessions to impersonate legitimate users. But, as suggested above, other, much broader malevolencies beckon. Effective cookie defense today requires a site to centrally screen all HTTP traffic for cookies and intercept them, and, to be doubly sure, require that cookies be disabled on the browsers of all client machines. The sum of these actions may both slow down the network and render popular web sites unusable; neither are likely to be popular with users.

Snoop (or spy) ware is mobile code, usually hidden in apparently innocent code and downloaded without the users knowledge or consent, that enables the snoop or spymaster to covertly monitor user activity, usually remotely. (The large number of qualifiers in the definition is reflective of the diversity of the snoop (or spy) ware. Some, such as the FBI's Magic Lantern, may be technically legal; whether a warrant, such as is necessary with wiretaps, is required is in contention. Nor does the snoop (or spy) code really need be mobile; it can be installed surreptitiously, as in a "black bag" job.)

Aside from snoop (or spy) ware's invasive nature, and its ramifications for civil liberties, is the huge number of surreptitious ways it can be distributed. Some web-site hosts allow software pop-ups, a piece of Java or ActiveX code that runs whenever a user launches the browser. These pop-ups can enable "one-click opt-install" downloads for users that click on them. In other cases, there are "drive-by downloads," where the users are not informed they are downloading an executable. Preventing this sort of mobile code-carried malware can be difficult. There even exist small, short-lived applets that run on PC clients capable of modifying a computer's proxy settings so that all of a host's Internet traffic first flows though a company's network. Finally, as with cookies, the necessary policy measures, disabling Java and ActiveX at both host and client levels, may be perceived as Draconian and unreasonably restrictive, and are likely to increase management costs.

Current Issues

The use of mobile code raises a number of obvious issues:

- Access control: Is the use of the specific code permitted?
- User authentication: How can valid users be identified?
- Data integrity: How can one ensure that the code is delivered intact?

- Non-repudiation of use of the code, for both the sender and the receiver
- Data confidentiality: How can sensitive code be protected?
- Auditing: How can one trace uses of mobile code?
- Compromise of security: Mobile code may be malicious.

Product/Technology Status

Today's commercial products for mobile code defense generally combine several of the technical approaches discussed above in a proprietary manner. Depending on the vendor, the packaging varies widely, with some running as a HTTP proxy server, others as add-on code in a mail server, and still others as features of a general-purpose, anti-virus, firewall package. **Finjan Software Ltd.'s SurfinGate** employs a firewalling approach and allows only applets deemed safe allowed to run [14,15]. **Digitivity's CAGE 2.3** divides Java applets into graphical actions and all others; the former are allowed to run on the client, the latter run in a sandbox [16,17]. As noted above, **Microsoft's Authenticode** employs a code signing system in conjunction with ActiveX and Microsoft's Internet Explorer browser, and is limited to that environment [18]. **Computer Associates' eTrust Defense Solution Set** includes the **eTrust Content Inspection** for mobile code**, and** employs both signature and code signing approaches [19]. **Trend Micro's InterScan AppletTrap** employs all three defense techniques. It blocks applets based on signatures and code signing, and attaches "watcher" codes to applets before they are released to the client. Applets are then monitored within a protected sandbox and immediately terminated if illegal operations are discerned [20].

Technology Insertion

See Sections 2.2.2, Intrusion Detection Systems, and 2.2.3, Malicious Code and Virus Detection Systems.

Future of Mobile Code Defense

With one authority characterizing mobile code as "the dominant paradigm in Web computing," several research and development efforts are underway to improve mobile code security [21]. In late 1999, the U.S. Defense Advanced Research Projects Agency (DARPA) funded Reliable Software Technologies (RST) $1M for two years to develop software assurance technologies, with Dr. Anup K. Ghosh acting as principal investigator [22,23]. Beginning in 2000 with a $150,000 grant from Microsoft, Cornell's Information Assurance Institute (IAI), directed by Dr. Fred Schneider, has been researching language-based security for mobile code. The IAI, working with researchers at the U.S. Air Force Research Laboratory in Rome, N.Y., has also received annual support of $1M from the Air Force Office of Scientific Research, as well as an additional $4.6 M over five years from the U.S. Department of Defense [24].

2.3 ISS Technology Area 3: Confidentiality

Confidentiality ensures that sensitive or classified information is held in confidence. It is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes, i.e., to any unauthorized system entity [RFC2828, Internet Security Glossary]. As noted in Section 1, one technology may support more than one technology area, and it can be seen in this case how the confidentiality concept interplays with other concepts such as access control and availability.

In the FAA environment, confidentiality had not been a major requirement for air traffic management. However, as needs and technology have evolved, confidentiality, confidentiality through encryption, and other security services provided through cryptographic functionality have become factors. Currently, there are needs for confidentiality that may be provided through cryptographic techniques with respect to the following:

- Computer and network security-related information across the FAA, including within the NAS
- Investigative activity associated with system certification or incident investigation
- Personnel records including employment and medical records
- Acquisition activities
- Information on and used by systems that address airport physical security
- Intelligence associated with threats to air traffic management, such as terrorism.

As encryption and cryptographic techniques normally provide these services, a wide assortment of associated and complementary technologies and functionality is invoked ranging from the broad provision of privacy, authentication, non-repudiation, integrity, and controlled access to the various approaches to key management, including the various PKI concepts. These associated and complementary technologies directly address other security requirements that invoke cryptographic processes but do not necessarily invoke confidentiality directly. These other requirements include:

- Data integrity, authenticity, and availability with respect to the operational NAS communications
- Data integrity, authenticity, and availability with respect to international ATC communications
- Data integrity and authenticity with respect to software transport over networks
- Access control, data integrity, user and data authentication with respect to remote maintenance and control of elements of the ATC system
- Key management across the entire FAA as encryption and cryptographic implementations spread

- Key management compatible with both the COTS/Open Source and the Aeronautical Telecommunications Network OSI-based PKI
- Data integrity and authenticity with respect to the various intranet/extranet relationships associated with FAA and NAS operations.

2.3.1 Encryption (and Cryptography)--Hardware and Software

Cryptography is a body of enabling technologies, primarily mathematical in nature, which facilitate techniques to provide security functionality and fulfill the realization of security objectives derived through the normal systems engineering processes. Security objectives could potentially include functionality such as confidentiality, integrity, authentication, non-repudiation, authorization, access control, availability, message or "data origin" authentication, entity authentication (identification), certification, receipt, ownership, time stamping, revocation, and key management.

Encryption technologies provide powerful techniques for the realization of these security objectives. Encryption technologies, however, are also complex and in many ways obscure. They will provide required security functionality only after the encryption and cryptographic techniques are integrated into an appropriate system of technology and user procedures.

Note that in some cases, techniques other than cryptography, (e.g., physical separation, U.S. mail, etc.) may provide these same security functions. Further, COTS "crypto" products are typically products that provide one or a number of security functionality sets and do so in a manner recognizably associated with cryptography.

Consistent with the interrelationships between these technologies and techniques and consistent with how industry tends to taxonomize "encryption" products, industry and generally accepted practices closely relate confidentiality with encryption and cryptographic techniques, and in turn encryption and cryptographic techniques with the following:

- Data, voice, and e-mail confidentiality products
- Database security products
- VPN products
- PKI, certificate-handling, and CA products and services
- Cryptographic cards and hardware (accelerators, PC cards, appliances)
- Crypto toolkits (software modules and libraries)

In some cases the "crypto" nature of the product is self-evident, such as a product that encrypts a plain-text data stream and produces a crypt-text output for the purposes of confidentiality. In other cases, this is not self-evident, such as the case where IPsec provides for only integrity and authentication checking in transport mode--thus the plaintext is always visible. The integrity is provided, however, through cryptographic manipulations of the data, even though nothing of the original message is encrypted. In other words, cryptography is used not to provide confidentiality, but only to provide integrity and authentication. This case is less self-evident.

Cryptography and cryptographic specific products can be categorized into constituent parts in a number of ways. One such breakdown would include the following:

- Symmetric algorithms (single shared secret-key algorithm such as the Data Encryption Standard [DES] algorithm)
- Asymmetric algorithms (public/private key algorithms, also known just as “public-key” algorithms such as the Rivest-Shamir-Aldeman (RSA) algorithm)
- Random number and pseudo-random number generation
- Hash functions
- Digital signatures
- Key-management techniques.

All cryptography and products that utilize cryptographic techniques, including those situations where confidentiality is being realized through the technique, have associated with them the ubiquitous problems of key management and key distribution. In other words, how does key material necessary for cryptographic-based interactions get distributed in a secure manner among participants in those interactions, especially when those participants are not co-located? This is not a problem with small-scale applications, but it is a huge problem at the enterprise level. PKI (Section 2.3.3.), and its use of public-key technology, is one attempt to address the key-distribution problem associated with widespread use of cryptographic techniques to provide the various security services.

In general, cryptography and cryptographic techniques provide for primitive security services such as privacy, authentication, and integrity. Product developers then incorporate one or a number of these security service primitives into products. A VPN gateway product may provide for a range of security services and functions, but many are built on the security service primitives, many of which in turn are built on top of cryptographic techniques and technology.

In general, the greater architectural and systems engineering context must be properly embraced and confidentiality requirements and cryptographic processes must be properly placed within that context. That context would include the following:

- Security policy
- Key management considerations
- User procedures

- User training
- Security architecture.

Federal Information Processing Standards (FIPS) PUB 140-2. Consistent with cryptographic modules or primitives (normally software) providing confidentially and other security services as part of products and techniques is the notion of third party evaluation of those cryptographic modules by an independent evaluator, based on U.S. Government sanctioned standards. Consistent also with this is the understanding that the cryptographic module is then incorporated into a product or technique. As defined by FIPS PUB 140-2:

- "Cryptographic Module" is the "set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary."
- The "cryptographic boundary" is an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

FIPS PUB 140-2, Security Requirements for Cryptographic Modules, provides the standards that developers and approved third-party evaluators must follow in order to achieve FIPS 140-2 approved cryptographic modules. The standards and requirements specify four security levels against which the module will be evaluated. Some requirements are shown below. Note, this is not a complete listing of the requirements for the various security levels.

- Use of varying degrees of approved algorithms
- Use of varying levels of authentication
- Evaluation to various Common Criteria evaluation assurance levels

It is very important to note that citation of FIPS PUB 140-2 does not guarantee a good security posture for a cryptographic product or system that is being evaluated. A security product or system can be badly made using a FIPS 140-2 approved cryptographic module in an otherwise poor security context. Citation of FIPS 140-2 does not equate necessarily to a strong security posture.

Advanced Encryption Standard. The NIST has issued FIPS Publication 197, dated November 26, 2001, which specifies the Advanced Encryption Standard (AES). The AES uses a cryptographic algorithm known as the Rijndael algorithm. The AES formally refers to this algorithm as the "AES algorithm."

With the addition of the AES algorithm, there are now four FIPS-approved algorithms for encryption:

- DES algorithm (FIPS 46-3)
- Triple DES algorithm (FIPS 46-3)
- Skipjack (referenced in FIPS 185 – Escrowed Encryption Standard)
- AES (FIPS 197)

The algorithm of choice would be the AES algorithm. Next would be 3DES. Skipjack has almost no use in the COTS/commercial world and DES should only be used where low-grade security is acceptable.

Other COTS and Industry Best Practices Algorithms. There are numerous cryptographic algorithms used within and by industry that represent industry best practices but do not represent formal standards-approved algorithms. In some cases these do not enjoy wide use; in other cases, they represent the de facto industry standard. Judicious selection of algorithms in light of acquisitions processes must consider the range of algorithms from standards-approved through industry-only de facto standards. This complicates many of the normal standards-based government acquisition activities, so care and consideration must be used when deciding these issues.

Key Management. There are activities currently going on within the NIST to facilitate appropriate choices with regard to key management techniques and technologies. These efforts are aimed at providing background information and establishing frameworks for key management to support appropriate decisions when selecting and using cryptographic mechanisms. Documentation exists in draft/working group form at present and covers the wide range of key management techniques including the two general approaches to key management identified as “key agreement” and “key transport.” The ultimate goal is to produce FIPS guidelines for key management.

Current Strengths

- Maturity: From the perspective of the cryptographic technology specialist, the state of cryptographic technology, with regards to commercial products, is fairly mature.
- Good understanding: Algorithms are fairly well understood and associated protocols are also fairly well understood.
- Agreement: Among those who know the subject area, there is much agreement on items such as algorithmic appropriateness, algorithmic strength, and appropriate technology.
- Powerful and useful: When applied by specialists, cryptographic techniques are extremely powerful and useful in enabling security technologies.

Current Issues

- Obscurity: A large problem, however, is that the body of cryptographic technology and literature in 2001 is extremely obscure. It is very difficult for the non-specialist to grasp and is non-intuitive in many cases.
- Critical details: The details are particularly critical and, if not understood, incorrect decisions may create huge technical and programmatic risks.
- Misrepresentation: Cryptographic concepts and technology details are often misrepresented, not just through non-understanding, but intentionally and officially. Overall, the field of cryptography is a very difficult field through which to navigate.
- Strength of algorithms: Cryptography is both art and science. The "art" is fairly well aware of what constitutes "strong" cryptographic techniques. The balance is between necessary security on the one hand and processing capability on the other. Balancing the strengths (or weaknesses) of cryptographic algorithms based on national or international policies will not be addressed here except to reference the fact that many national entities have, or have had, import and/or export and/or possession restrictions placed on cryptographic-based products based on the strength of the underlying algorithm. The stronger the algorithm, generally the more restrictions placed on it.
- Key distribution and management: As noted earlier, key distribution and key management is still a very difficult aspect of cryptographic-based technologies. PKI is one attempt to address this. A PKI coupled with appropriate PKI enabled applications will mitigate some of this problem as long as all participants exist within a consistent and specific security domain.
- Compatibility between algorithms and implementations: National and international standards involving cryptographic products and technologies are still not readily available in spite of claims otherwise. In many cases, attempts are either stalled or overtaken by events. As a result, there are still many compatibility issues between algorithms and implementations from different vendors.
- Legal issues: In some nations, such as the U.S., cryptographic-based products are/were treated as munitions for the purposes of import, export, and possession. This complicates the market for cryptographic-based products and requires product quality considerations not normally found in other IT products. Vendors want to produce products technologically compatible across national boundaries. This impacts the quality of those products.
- Patent and trademark: Many algorithms are not open for non-moderated use. Patents and trademarks are held on many of the most used algorithms. The status of patents also is an issue, adding to a vast complication of already difficult issues.
- Key recovery and key escrow: Key recovery and key escrow technologies are those technologies that provide visibility into otherwise secure communications by duly authorized officials of government entities. This is generally accomplished through the provision of techniques or procedures that would make key material available to those authorized parties in a manner that would allow for covert, third-party, real-

time, and ubiquitous access to those otherwise secured transactions. This technology has touched almost all government sponsored activity in the area of cryptographic technologies for the general public. This impacts the strength of the cryptographic technique used, the complexity of administration and management, and the development of formal international standards.

- Open source solutions: A large collection of cryptographic applications exists as Open Source Software, circumventing many legal and commercial issues. Some applications are very significant within academic, commercial, and government communities, and must be so noted.

Technology Insertion

Encryption technology is mature and could be inserted into the FAA environment today. The challenge of encryption in an organization the size of the FAA may be the key management issue. As with PKI, there must be an infrastructure in place to support this technology. However, if the data confidentiality requirements warrant it, encryption is an important addition for information assurance.

Future of Encryption

The overriding goal of cryptographic technology is to make the use of cryptographic processes as invisible as possible to the actual users while still maintaining the strength and appropriateness of the algorithm and technique. Procedure, architecture, and processes are as important if not more important than the actual root cryptographic technology. Indeed, procedural, structural, and architectural errors and “social engineering” may represent the single largest threat and vulnerability mechanisms to cryptographic-based systems.

The U.S. Government, through the NIST, recently selected the algorithm that may eventually replace the DES algorithm. The new standard is based on a new open source algorithm called the AES algorithm and is referenced above. It is anticipated that many U.S. crypto products will support the new standard, which will provide improved encryption strength. At present, support for this algorithm is not as great as it currently is for DES and 3DES, but it is anticipated that support in the COTS arena will grow.

An expected trend is an increase in the overall use of crypto-based products. As Internet-based applications proliferate, the need for secure communications and transactions will increase. The primary drivers for Internet security are e-commerce applications.

2.3.2 Virtual Private Networks (VPNs)

A VPN creates a tunnel, a virtual channel, or a point-to-point connection across a shared or public network by encrypting the packets before they are sent out on to the network and decrypting them at the destination after they come out of the network. This process is usually transparent to the user. VPNs allow organizations to extend their network service over the Internet to branch offices and remote users creating a private Wide Area Network (WAN) via the Internet. Communication links can be done quickly, cheaply, and safely throughout the world.

A VPN is a blend of security technologies to secure network traffic as it flows between two or more endpoints. This is achieved by first authenticating the involved parties and then encrypting the data sent between them, thus ensuring confidentiality and integrity. Security mechanisms keep the IP network virtually private by keeping unauthorized users out of specified sites and encrypting data to prevent eavesdropping. Sending encrypted network traffic is the essence of VPN solutions and is referred to as "tunneling." Tunneling routers are used that are capable of routing network traffic by encrypting it and then encapsulating it for transmission across an untrusted network.

The usual means by which the information is sent securely is the use of a tunneling protocol (described later) through one or more ISP networks. The tunneling protocol and other security mechanisms can be managed by server or firewall software on the user site. Recently, ISP carrier networks have been deployed that provide many or all of these services in a separately defined IP backbone, with the intent of improving performance by decreasing router hops through multiple carrier networks.

The three categories of VPN solutions and their corresponding configurations are:

- Host-to-gateway: Remote access from a user to corporate servers (i.e., connecting to a server via a local ISP instead of dialing long distance via modem)
- Gateway-to-gateway or intranet: Connection between two or more sites within a corporation (e.g., a connection between two branch offices of the same corporation)
- Host-to-Host or extranet: External connection between different enterprises for collaboration and data sharing.

The market forces driving the adoption of VPNs are building daily, as the workforce is becoming increasingly mobile and distributed. ISPs hoping to capitalize on this growth market must build a tunneling infrastructure to support remote access VPN services. However, the primary and fundamental design question for the development of a tunneling infrastructure is deciding which protocol to consider.

VPN protocols. There are two major tunneling protocols used for VPNs. They are the Point-to-Point Tunneling Protocol (PPTP) and IPsec. A third protocol, the Layer 2 Tunneling Protocol (L2TP) has been used extensively in carrier networks and is starting to make its way into enterprise networks. Each protocol offers unique features and the utilization of any particular one has specific implications on VPN deployment. There is no standard for implementing VPNs, i.e., there are no documents that establish engineering or technical requirements for developing interoperable VPN solutions.

- PPTP (Layer 2 Tunneling): This protocol was originally developed to let remote users communicate securely over the Internet. PPTP is the most commonly used

VPN tunneling protocol. The reason for PPTP's success is its availability among products and vendors. While this protocol is not defined within an IETF standard, VPN implementations using PPTP will, in all likelihood, interoperate. Nearly all vendor implementations of PPTP have been written to work with Microsoft's implementation.

Another advantage in using PPTP is that, unlike IPsec, PPTP operates at the datalink layer (Layer 2 of the OSI model), which is beneath the network layer. This allows different networking protocols to run over a PPTP tunnel.

PPTP is easier to deploy than IPSec, but provides much weaker security. Still, PPTP tunneling may meet the needs of many small-to-midsize businesses. Even though IPsec and L2TP have been added to Windows 2000, Microsoft plans to continue supporting PPTP.

- IPsec (Layer 3 Tunneling): IPsec was developed by the IETF as a set of protocols that offered IP security features within the IP network protocol. There are a large number of security services offered with IPsec. For instance, it can be used to encrypt and authenticate data that is to be transmitted over the Internet or a service provider's network. IPsec also makes use of digital certificates to provide a more robust way to authenticate users.

  One of the attractions of IPsec is that it gives IT managers a lot of flexibility in how VPN sessions are secured. Essentially, a network manager must define what is called a Security Association, which specifies what is needed for a user or site to establish a connection through an IPsec session.

  The things that are specified in a common Security Association include: what encryption algorithms will be used, how the two nodes will exchange encryption keys, and how long a particular key is valid. The association also includes what authentication algorithms are to be used and the lifetime of the Security Association.

  Large businesses that require stronger encryption and authentication may pay the premium price required to build an IPsec infrastructure. IPsec remote access support varies from product to product.

Current Strengths

Aside from direct cost savings, using a VPN can have secondary cost benefits, such as greater mobility. With VPNs, employees can connect from anywhere they can make an Internet connection and with the same procedures they use in the office.

- Access: Remote users can access corporate network services and resources with the same efficiency and functionality as if they were in the office.

- Improved connectivity: It offers business partners improved connectivity (e.g., file sharing, e-mail, mobile clients). Business partners can connect to each other's networks, allowing for shared proprietary information on joint projects.
- Enabling support: VPNs also support collaboration and efficient electronic communication and commerce.
- Cost savings: Avoids leasing and managing dedicated lines; very cost effective means for private communications.
- Flexibility: Permits remote access infrastructure within ISPs; there is a lot of flexibility in the types of configurations and number of endpoints.
- Security: Provides a high level of security using advanced authentication and encryption techniques.

Current Issues

There are four approaches to building VPNs: router add-ons, firewall upgrades, dedicated servers, and stand-alone VPN devices. The router-based solution is fairly simple and entails a quick download from a vendor's site and updating the router software. Typically, the software adds firewall, encryption, and tunneling features to the router's functionality. The drawback to this approach is that the VPN is software-based and routing performance can be affected negatively.

Upgrading firewalls to create a VPN is cost effective and avoids the incompatibilities that arise from using firewalls and VPN appliances together that are produced by different vendors. Unless the firewall was designed to include VPN capabilities, the firewall's performance will be affected negatively due to the encryption and tunneling processes added to its functionality. As with routers, virtually every firewall vendor offers VPN services as an option. Firewalls may constrain the total number of tunnels supportable by the router/hub. Firewalls are good for extending a hub and spoke WAN/VPN, but they are not so good for a peer-to-peer network environment needed by many individual tunnels.

A number of issues with VPNs present management challenges, especially for extranets and implementations for a large number of users. Some of the issues related to deploying VPNs are centralized management, scalability, interoperability, and performance degradation on networks. These issues are developed below.

- Centralized management: The technical aspects of deploying a VPN are only part of the solution. Client policies and configurations must be developed, maintained, and enforced. Managing keys and certificates is an issue unto itself, particularly as the number of users increases and updates and revocation of certificates are required. Deciding who has the authority to validate certificates between enterprises is an important companion issue.

  Management of shared secrets is also critical. Passwords, digital certificates, tokens, smart cards, and biometrics are all different means to authenticate users to a VPN. What is needed is the ability to support the same policies on both ends of the VPN. This includes such things as the minimum level of encryption that must be used, what mechanism to use for key exchange, and whether or not to accept a digital certificate offered by one device to the other.

- Scalability: VPNs becomes progressively more cumbersome to manage as the number of nodes increases. The VPN community for a given enterprise is very dynamic. The scalability issue is further complicated by the type of environment that the VPN must accommodate, e.g., a few/finite number of sites with greater bandwidth or many/mobile sites and less bandwidth.

  Shared directories among sites are created and changed for evolving business needs. Many of the existing VPN devices are not designed to operate very efficiently with the larger number of nodes. As more sites and more users are added, it becomes progressively difficult for the VPN device in the central location to handle the additional load of encryption and tunneling tasks. Load balancing and fail-over (redundant VPNs) are essential for large implementations. Management of keys, policies, and equipment become increasingly complex. Because IPSec operates on the network layer (OSI Layer 3), it is inherently more scalable than the other protocols (PPTP, L2TP). That is why IPSec is growing in popularity as the standard VPN protocol. Network layer encryption prevents eavesdropping or tampering with data across a network during transmission.

- Interoperability: Solutions may be difficult to design if incompatible products using different tunneling protocols are used. Even among interoperable VPN products, design and implementation can be a challenge. Many IPsec interoperability problems stem from users not knowing how to set up the equipment. Network managers need the instructions to configure the products, as well as the assurance that the products will work together (using ICSA IPsec-compliance testing). ISCA IPsec-compliance certification does not guarantee compatibility; the VPNs need to be configured properly.

- Performance degradation: Caution should be exercised in designing VPN solutions. The use of older firewalls and routers may decrease performance since they were not designed to handle today's higher rates of data transmission, especially with the advent of optical networks and high-speed connectivity, such as Digital Subscriber Lines (DSL) and cable modems. Newer VPN integrated solutions, however, include optimized, interoperable firewalls and routers, which will not result in a measurable degradation of performance. In these cases, the processing overhead is expected to be from 2 to 3%. Prototyping is strongly recommended due to the number of variables.

- Regular communication: Due to the need to maintain a connection-oriented communication stream, VPN connections may not be suitable for links that have high rates of flap (i.e., on-off communication) or sporadic delay (e.g., microwave/satellite).

- Tunnel endpoints: Because VPN tunnels may be implemented on a large variety of devices, e.g., routers, firewalls, dedicated appliances, or servers, it is possible to create many similar, router-to-router tunnels very quickly. This creates the potential for excessive control traffic clogging WAN links or incomplete implementations of security where some connections are secure while other portions are not. Early planning and management of tunnel creation can mitigate these risks as well as minimize the total number of tunnels that are needed throughout the network. In scenarios where many, e.g., hundreds of, users need VPN access tunnels, these tunnels should be aggregated. In other scenarios where true endpoint-to-endpoint, i.e., final user, encryption is essential, or where only a few users, e.g., less than 10%, need VPN access, then software tunneling programs such as L2TP may be better suited. Also, if there are two secure locations (endpoint-to-endpoint) from LAN to LAN, the router-based VPN can be created to authenticate the sites, but not the users.

Ongoing R&D

- VPN Labs (http://www.vpnlabs.org/): Offers on-going research, reviews, and a discussion forum for VPNs. It also tests VPN software, hardware, and services.
- SANS Institute (http://www.sans.org/): The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions to the challenges they face.
- VPNC (http://www.vpnc.org/): Virtual Private Network Consortium (VPNC is a trade association for manufacturers in the VPN market.

VPN solutions combine various security technologies and products (e.g., routers, firewalls, and encryption software). VPN research really means research in the various components of VPNs. More important than research is the need for standards that will be embraced by all vendors across all platforms. Key management is another major issue for VPNs, so research on PKIs will be relevant. Research is currently being conducted on the use of parallel VPN devices and Quality of Service (QoS) services to address performance and scalability issues.

- Parallel VPN devices: Research is ongoing in the area of parallel VPN devices that are able to perform load balancing sessions between them and provide back-up service in the event of a device outage. When the ability to connect to multiple VPN devices is offered and one device fails, the user will be connected automatically to the remaining working device when establishing a session.
- QoS-based services: VPNs are far less predictable than dedicated links in delivering consistent performance. For VPNs using an Internet backbone, performance delays are at the mercy of multiple ISPs, not the enterprise. Service level agreements on latency do little to assure users that they will not experience VPN-related delays. However, on premium ISPs, network managers are beginning to see the rollout of true QoS-based VPN services.

  QoS-based VPN services take the bulk latency guarantee on a provider's backbone and give IT managers more control over their VPN traffic. These services let the IT manager decide which traffic gets priority. Typically, a bandwidth manager tool sits at the edge of the corporate network, collecting information about the traffic passing over a link into the provider's network. The information includes the type of traffic, which applications generated the traffic, which users generated the traffic, and the source and destination addresses for the traffic. The data is analyzed to identify when and how much bandwidth is used by individuals, groups, and applications (e.g., web surfing during the lunch hour). Different links and bandwidths are created based on need. Bandwidth is managed based on usage, and priorities may be set as to which applications and users get access and when they are likely to get that access.

Leading Organizations

The number of VPN device announcements is growing at a staggering rate. The proliferation of IPsec implementations, the differences among PPTP, Layer 2 Forwarding and L2TP, and the need to determine the correct placement of VPNs make it all the more confusing. Further complicating matters, solutions must not only suit current requirements but must be adaptable to future needs.

An excellent source of up-to-date information on VPNs is the VPNC, http://www.vpnc.org/. VPNC is the international trade association for manufacturers in the VPN market. VPNC will not create standards; instead, it will strongly support the current and future IETF standards. The primary purposes of the VPNC are:

- Promote the products of its members to the press and to potential customers
- Increase interoperability between members by showing how the products interoperate
- Serve as the forum for the VPN manufacturers throughout the world
- Help the press and potential customers understand VPN technologies and standards
- Provide publicity and support for interoperability testing events.

Product/Technology Status

VPNs lower costs by eliminating the need for expensive long-distance leased lines. An amazing amount of development effort has been invested in VPN technologies. Yet the task of choosing and deploying a VPN solution remains far from simple. The most common public network used with VPNs is the Internet, but traffic congestion and router failures on the Internet will adversely impact the performance of VPNs. When building an Internet-based VPN, it will be important to choose a high-quality service provider.

The leading VPN companies and their VPN products are:

- Altiga C10 from Altiga Networks, Inc.: http://www.altiga.com
- Intel Shiva LanRover VPN Gateway Plus: http://www.intel.com/network/shiva

- Lucent VPN Gateway: http://www.lucent.com/products
- TimeStep Permit/Gate 4620: http://www.timestep.com
- MCI VPN networks: http://www.vpnetworks.com
- VPNet VPNware VSU-1010: http://www.vpnet.com
- VPN-1 Gateway: http://www.checkpoint.com/products/vpn1/gateway.html
- Nortel Networks: http://www.nortelnetworks.com/index.html
- Cisco Systems: http://www.cisco.com/warp/public/44/solutions/network/vpn.shtml

Technology Selection Considerations

1. Criteria that could be used to evaluate and compare VPN technologies:

    - Network types supported by the VPN (i.e., remote access, intranet, or extranet)
    - Flexibility of VPN solution to accommodate dynamic environments
    - Interoperability: Conformance to standards on tunneling protocols (IPSec, PPTP, L2TP)
    - Number of nodes supported by the VPN solution; VPNs becomes progressively more cumbersome to manage as the number of nodes increases
    - Bandwidth and network throughput requirements (e.g., a few/finite number of sites with greater bandwidth or many/mobile sites and less bandwidth).
    - Type of OS platforms supported by the VPN solution

2. Current performance considerations:

    - For interoperable and secure VPNs, the protocols required should be one of the following:
        - IPsec with encryption: IPsec is by far the most dominant protocol for secure VPNs.
        - L2TP inside of IPsec: L2TP running under IPsec has a much smaller but significant deployment.
    - Number of nodes supported: anywhere from a few to thousands.
    - Prices for VPNs range from $4995 (for 25 nodes) to $49,995 (for 1000 nodes) plus $11,995 per another 1000

3. Evaluation and testing considerations:

    - Before selecting a VPN product, an overall information security architecture is required. The architecture will specify the external access points of the enterprise network. VPNs then must be designed for those access points in order to implement remote access by authorized users. Program managers also need a strategic plan to bring VPN services into the deployment from all tactical and strategic vendors. Establishing a VPN involves compatibility testing of every application and operating system that employees use on the VPN.

- Select a product carefully and stick with it for the particular network configuration (e.g., an extranet) in order to mitigate interoperability issues.
- Although knowing which products conform to the IPsec standards is important, program managers need to know which products interoperate with other products in order to make technology choices.

Technology Insertion

The VPN technology is beginning to be used in the FAA today. The extent of VPN use in the future is a question of requirements. For FAA applications that use shared or public networks, VPNs can help keep costs down and still provide secure communications. However, performance is dependent on the service provider of those networks, and this requirement must be kept in mind.

Future of VPNs

Market research firms and vendors are predicting that the worldwide market for VPNs will reach, if not exceed, $10 billion by 2003. Conservative estimates show a growth rate of 300%, while other predictions show a growth rate of up to 1000%.

Research is still needed to provide more control of performance on the provider's network. The next evolutionary step of QoS-based VPNs would give network managers the ability to use tiered levels of service for even more control. For example, a bandwidth management tool could be used to classify traffic and then link self-defined priority levels to differentiated services offered by a service provider.

The IETF Differentiated Services Working Group is exploring ways to accomplish access prioritization. There has been progress on IETF standards that try to match traffic classifications on the enterprise network with services of different quality on the WAN side. Some service providers would like to centralize all security and bandwidth management functions of a VPN into the core of their networks. Essentially, the idea is to adopt a network-centric approach to providing enterprises with managed VPN services rather than relying on customer premises equipment. One advantage is that no special equipment is required in the corporate network. Providers would simply use a WAN router or packet-forwarding device within the enterprise.

2.4 ISS Technology Area 4: Integrity and Non-Repudiation

Integrity ensures that data cannot be altered from their source without detection. This includes accidental or malicious modification, alteration or destruction.

Non-repudiation is the affirmation, with extremely high confidence, of the identify of the signer of a digital message using a digital signature procedure. It is intended to protect against any subsequent attempt by the signer to deny authenticity. Non-repudiation aligns closely with integrity (and to a lesser degree, authentication). It enables a recipient of a message to prove the identity of the source of the message, and do so to the satisfaction of an independent third party. In the FAA environment, this is one of the ISS areas of greatest importance to the NAS.

2.4.1 Logging and Auditing

Besides system backups one of the most elementary and oldest practices to recover from accidental misuse and malicious intrusions to a non-networked computer is the practice of using system programs (computer OS utility programs) to record security-relevant events onto one or more log files (text files stored in the computer). The technology implementing this practice is called "login and auditing" and it has not only a contingency response value but can be a deterrent to careless or malicious use of the computer, because it can provide a reliable record of user/intruder steps leading to and causing a computer incident. Thus early UNIX systems would record who logged in, who logged out, what files were added or deleted, and what files changed either in content or access permissions. When a problem occurred, the log files could be examined i.e., "audited," to investigate the cause of the problem. Logging and auditing operates on two architectural bases:

- <u>Client-sensing architecture</u>: In auditing systems based on the client server architecture, clients at monitored workstations collect logging events and upload them to a server workstation. This architecture mitigates the threat of destruction and modification of the log files by removing them to the server platform, one step further from potential attackers and which can be further protected against intrusion. The client server architecture also mitigates the risk of running out of storage space and crowding out the workstation principal application.
- <u>Sensor-director architecture</u>: If the clients at monitored workstations, in addition, perform a first level of audit processing and send alarms to the server workstation, the auditing system becomes a bit more proactive or at least a system with instantaneous reaction time. This type of audit system is said to be based on the sensor-director architecture. The director (server) workstation in addition to receiving alarms from the sensor would also ideally receive the original unprocessed "native" log files from the monitored workstations at off-peak times. It is important to preserve the native logfiles because they may be required in criminal prosecutions. The director workstation should also perform correlation of alarms and a second level audit on the events of the native log files applying a variety of analysis methods including pattern recognition.

<u>Current Strengths</u>

- <u>Increased capabilities</u>: As the practice of networking computers became widespread and networking services delivered via system programs and applications multiplied, the threat of malicious and unintentional threats increased as well and so did the logging and auditing capabilities to help counter misuse of the new capabilities. In fact this process can be characterized as a race between the emergence of new threats and actual attacks to the evolving networked environment and the redesign and addition of new features to auditing systems to help counter them. Thus in addition to recording user logins and file access operations, system programs and applications have been extended to log usage of networking services such as transferring a file, establishing and managing remote sessions, and browsing web sites.

- Network management: It should also be noted that the usefulness of logging and auditing in a networked environment is not restricted to services and applications running on a workstation end system. The usefulness of logging and auditing also extends to network management application processes running on intermediate systems such as routers and switches as well as network management workstations.

Current Issues

Traditional logging and auditing systems have four notable limitations.

- Storage space: First the log files can consume large amounts of computer storage space.
- Analysis difficulty: Massive amounts of logged data make the task of analyzing it very difficult.
- Vulnerability: The log files are vulnerable to modification or destruction.
- Reactive nature: Auditing is a reactive rather than a proactive tool.

The different attempts by industry to address these limitations have produced increasingly sophisticated products that take advantage of the client server architecture and exploit other technologies notably intrusion detection and pattern recognition.

Ongoing Research

As the basic limitations of the early logging and auditing technology have been comfortably overcome, there is no notable ongoing R&D. However, since this technology relies on the identification of incident indicators of user actions and data, it can benefit from research in the areas of pattern recognition, data mining, and anomaly-based intrusion detection.

Product/Technology Status

Analysis of logged events was deficient in self standing log/audit systems for a long time but this has changed in the last few years and many commercial off-the-shelf (COTS) products now apply many methods to analyze logged events and provide many added value such as intrusion detection, incident response and forensics. A review of a number of COTS logging/audit tools is shown in Table 2.8 below from a MITRE paper “Compendium of Commercial and Government Tools and Government Research

Projects" by Leonard J. LaPadula. A review of the eTrust Audit tool from Computer Associates International is added to the review list following the same format and criteria adopted by LaPadula, i.e., based on vendor claims and complemented with other sources of information, when available and edited for uniformity of style.

Technology Insertion

The FAA should be using logging and auditing tools in its environment now.

Table 2.8 COTS Logging/Auditing Tools

Product Name	Vendor	Tool Type	Architec-ture	Sensor Platforms	Director Platforms	Methods of Detection	Data Sources	Reactions	Communications
PreCis 3.0	Litton PRC	System Monitor; host based audit management and misuse toolkit	Sensors-Director	HP-UX, Windows NT, Sun Solaris, SCO CMW+	HP-UX, Sun Solaris	Pattern matching (Agents & Director); Statistical deviation detection (Director)	Audit data in monitored systems; central location for analysis and archiving	Alerts	Provides authentication for connections and non-repudiation support for data transfers
Kane Security Monitor for Windows NT	ODS Networks, Inc.	System Monitor; based on event log analysis for Windows NT networks	Sensors-Director	Windows NT, Workstations and Servers, Intel-based systems only	Windows NT, Workstation or Server, Intel-based systems only	Pattern matching	Windows NT security log, applications log, and systems log; centralized collection facility	Delivers alerts for management systems consoles as SMTP alerts	Security verification process takes place between agents and KSM manager
Computer Misuse Detection System (CMDS^{TM})	ODS Networks, Inc.	System Monitor; provides both intrusion detection and misuse detection in a single system	Sensors-Director	Sun Solaris 2.5 or higher, HP-UX 10.x DG/UX B2 with Security Option 4.12, Trusted Solaris 1.x, Windows NT 4.0	Sun Solaris 2.5 or Higher, HP-UX 10.x, DG/UX B2 with Security Option 4.12	Profile user behavior, identifies suspicious activity, detects intrusions and misuse of resources through data analysis	Audit data generated from hosts, servers, firewalls, IDSs, routers and wide variety of applications		

Product Name	Vendor	Tool Type	Architecture	Sensor Platforms	Director Platforms	Methods of Detection	Data Sources	Reactions	Communications
eTrust Audit	Computer Associates International	Enterprise Auditing Tool	Sensors-Director; multi-tiered architecture; recording and routing agents installed on each targeted system and a server collector to consolidate data	UNIX, Windows NT	Windows NT	Pattern matching	Windows NT security log, UNIX systems logs, and applications log	Any specified user in enterprise network can receive alerts, mail, scripts, and system status notification	Can transmit events securely through firewalls or across the Internet in encrypted form

2.4.2 Data Mining for Intrusion Detection

Data mining is an approach to evaluating data to discover or gain valuable insights, especially those that would not be readily apparent or obvious from superficial, traditional, or isolated examinations of data. Data mining is an interdisciplinary field and uses pattern recognition, statistical and mathematical techniques.

The concept of data mining is not new, and comes from the generic definition of the verb "mine:" to seek valuable material in; to burrow beneath the surface of [25]. Data mining uses and sifts through disparate data bases, often in data warehouse or data mart storage environments. By sifting through these large amounts of stored data, data mining can discover previously unknown and meaningful data relationships, i.e., valuable material, beneath the surface. While the concept is old, data mining has new uses as the technology (databases, faster computers, more efficient storage, etc.) makes it easier to perform the data evaluation, especially with large amounts of data.

Data mining differs from traditional data analysis in data mining's capability to discover information without a previously formulated hypothesis. With traditional data analysis techniques, the user or analyst provides inputs such as analysis criteria, hypothesis and/or factors influencing the outcome. By contrast, data mining would start without these kinds of inputs and try to discover or identify what were the influencing factors. As an example, data analysis might start with the hypothesis that the number of failed login attempts is an indicator of intrusion attempts and then count the number of failed login attempts. Data mining would not start with a hypothesis but rather would examine a larger set of data to discover hypotheses that are supported by the data, i.e., factors correlated with system intrusion.

Data mining and data analysis can complement each other. Data mining can discover possible actionable information or possible hypotheses. Data analysis can then act on the results of the data mining by refining a hypothesis or further analyzing the data using different analytical techniques, such as statistical analysis.

Data mining has applications in any domain that has large quantities of data. Some applications include information assurance, law enforcement, medicine and customer-based marketing. Within information assurance, data mining is finding a potentially strong application in the area of intrusion detection. This chapter will focus on the intrusion detection application.

Typical IDSs are designed and implemented based on the understanding of known threats, whose patterns are sometimes called "signatures." Threats are frequently invented/re-invented, and the IDS builders respond with specific system updates against the specific new threats. The IDS builders' job is difficult because of the frequency and number of new threats, the increasing complexity of systems, and the increasing amount of data that must be analyzed to identify and understand the new threats in order to construct new defenses. The system under attack is vulnerable during the lag time between identification of a new threat and the deployment of a defense against it.

Data mining is expected to be able to improve IDSs in these key areas:

- Efficiency: While testing known signatures is fast, sifting through data to identify threats and develop new signatures in a reasonable time frame is difficult for human analysts. With so much data, it is easy to overlook some parts of the data or misinterpret its relevance. Data mining can automate the sifting of the data, allowing larger amounts of data to be examined more thoroughly in a shorter period of time, and present results for the analyst to evaluate.
- Profiling: Profiling can be used to determine the normal bounds of network activity and uses of information systems. Deviations from these normal bounds are indicative of intrusion. Data mining enables profiling individual systems, whose behavior may vary due to local conditions, site specific adaptation, or even individual users. The resources for human-developed profiles at a fine-grained level are not available – data mining is the only way such profiling will be practical.
- New threat identification: Currently the typical IDS uses known signatures to identify known threats. The signatures are often specific to the known threat and the specific computer or network system. The IDS typically does not generalize from the known signature to be able to detect a new threat that has a different signature. Data mining can be used to detect anomalies – behavior that has not been seen before, but is likely to be a new threat.

Current Strengths

- Data reduction ability: As computing environments increase in size and complexity, the amount of information that describes their operation has increased to the point that it is difficult, if not impossible, to analyze and understand that information without good tools. Data mining can be used to identify which data elements are most useful in predicting or gauging the threat level of generated alerts.
- Discovery capability: Data mining can provide insights from that data that might not be apparent using more traditional tools, i.e., be able to detect new attacks that hand-crafted methods tend to miss. This capability derives from the large amount of data used and the interdisciplinary use of a variety of tools and techniques, including visualization tools to present the information.
- Potential for real-time predictive capability: As a result of evaluating past and current system behavior, data mining can make predictions about future behaviors. The importance of this for intrusion detection will be the ability to discover patterns of behavior that indicate an attack is starting or getting ready to start. Such discovered patterns can be used to enable defensive action before serious damage can occur.

Current Issues

- Data selection: While data mining requires analysts to be more inclusive in deciding which data is to be searched, limits still exist. There must be a balance and trade-off on selected data. Large amounts of data will take time and computing resources to search and will not always guarantee the best models. Small, selected data sets may result in better models (especially if the additional data represents older attacks or alerts that are no longer threatening), but may also be so small as to miss important patterns. Making appropriate data selection choices is normally evaluated by evaluating the resultant model.

- Data preparation: This is often the most time consuming task of data mining. Some estimates are as high as 60% of the project time. Because the data being mined often comes from a variety of sources and formats, considerable effort may be required to organize the data, find appropriate ways to express the data in formats appropriate for the given data mining procedures, and standardize data definitions and taxonomies.

- Domain specificity of data: Since each data mining initiative is using data specific to the project, the data mining effort is usually custom to the project and the cost of labeling the data must be incurred for each deployment of a data mining project. The customization effort in turn increases the level of effort to finally get results.

- Data quality: As with any data analysis-type effort, the results are partially dependent on the quality of the data being used. Data mining often uses data from multiple sources, and the data quality standards may differ among the various sources. Poor data quality standards from even a single source may undermine the quality of the data mining results.

- Computing time and cost: The computing time and cost may be considerable for data mining because of the large amount of data being processed, the types of tools being used and the nature of the work itself. Data mining often uses graphical and visualization tools to present the results to the analyst, and these tools sometimes require extra computing resources. The sifting of data often requires multiple processing iterations to develop results. The complexity and scope of the search that data mining systems perform is a major barrier to discover new models of attacks in real-time. (Note, however, this does not imply that developed models cannot be deployed to process audit data and detect intrusions in real time.)

- Accuracy of results: Data mining is usually an open-ended type of processing activity without much guidance or a hypothesis. After all of the processing, the results still have to be evaluated by a subject matter expert to weed out meaningful patterns from the obvious, and to avoid pitfalls of mistaking correlation and causality. Also, data mining-based IDSs typically have higher false positive rates than traditional handcrafted signature-based methods, making today's systems unusable in real environments.

- Speed or availability of results: Because of the large amount of processing, data mining results may not be available quickly. For intrusion detection events, data mining should be able to provide post-event analysis, but may not be fast enough with today's technology to meaningfully forecast potential intrusions.

- Data storage: Data mining initiatives require large data storage, especially for network data. Even a small network generates potentially terabytes of data. Using off-line storage may be satisfactory for post-event data mining, but may not be adequate for faster processing to attempt to forecast future events.
- Data collection: Data mining initiatives may not be able to access needed data due to privacy laws or data ownership issues. If, for example, an organization has not informed employees that computer systems are subject to monitoring, and has not detailed the legal rights of the company in this regard, the data mining initiative may not be able to collect the relevant computer system and/or network data. The data mining initiative may have to go through an administrative process to access data in the case of data ownership issues.

Ongoing R&D

- Computer Science Department, North Carolina State University, Raleigh NC, 27695, contact: Wenke Lee: wenke@csc.ncsu.edu
- Computer Science Department, Columbia University, New York, NY 10027, contact: Salvatore J. Stolfo, Eleazar Eskin, Matthew Miller, Shlomo Hershkop, and Junxin Zhang: {sal,eeskin,mmiller,sh53,jzhang}@cs.columbia.edu
- Computer Science Department, Florida Institute of Technology, Melbourne, FL 32901, contact: Philip K. Chan: pkc@cs.fit.edu
- Department of Information & Software Engineering, George Mason University, Fairfax, VA 22030, contact: Daniel Barbara: dbarbara@gmu.edu
- Electrical and Computer Engineering Department, Purdue University, West Lafayette, IN, 47907, contact: Terran Lane and Carla Brodley: {terran,brodley}@ecn.purdue.edu.
- IBM T.J.Watson Research Center, Hawthorne, NY 10532, contact: Wei Fan: weifan@us.ibm.com
- The MITRE Corporation, McLean, VA 22102, contact: Bill Hill: bill@mitre.org
- Information Systems Technology Group, MIT Lincoln Laboratories, Lexington, MA, 02173, contact: Oliver M. Dain: odain@sst.ll.mit.edu or Dr. Richard Lippmann

Leading Organizations

The ACM Special Interest Group on Security, Audit and Control (SIGSAC), http://www.acm.org/sigsac/. The SIGSAC addresses all activities involved with maintaining and protecting computers and their programs, focusing on the architectural foundation of secure systems and development of standards. SIGSAC sponsors a number of conferences, the most strongly data mining-related is the Conference on Computers and Communications Security.

The ACM Special Interest Group on Knowledge Discovery in Data (SIGKDD): http://www.acm.org/sigkdd/. The SIGKDD annual conference is the premier event for research in data mining.

KDnuggets: http://www.kdnuggets.com/. This site provides a wealth of updated information related to data mining, including commercial tools, upcoming conferences and publications.

The Data Mining Group (DMG) is an independent, vendor-led group that develops data mining standards, such as the Predictive Model Markup Language (PMML). PMML is an attempt to standardize the descriptions of predictive models so that analysis algorithms can be shared between applications from different vendors. Given the lack of specific tools for data mining in intrusion detection, and the immaturity of existing commercial tools, this effort is important.

Center for Education and Research in Information Assurance and Security at Purdue University (CERIAS): http://www.cerias.purdue.edu. CERIAS is a multidisciplinary research and education center in areas of IS (computer security, network security, and communications security), and information assurance.

Advanced Technologies for Information Assurance and Survivability (ATIAS) out of Wright-Patterson Air Force Base: http://www.afrlsn.afrl.af.mil/index.html. The ATIAS program conducts R&D in all aspects of information assurance, but is most focused on short-term studies. Work is sponsored by DARPA's Information Processing Technology Office: http://www.darpa.mil/ito.

Product/Technology Status

While commercial tools for data mining exist, they are generally directed toward marketing and financial markets. There are no consumer products aimed specifically at security issues. The data mining tool market place is rapidly changing, with frequent entry of new vendors and departure of even established companies. Table 2.9 gives some of the current leading tool vendors.

Table 2.9 Current Leading Tool Vendors

Product Name	Vendor	Tool Type	Platforms	Mining types
Intelligent Miner for Data	IBM	Toolkit for building data mining applications	AIX, OS/390, OS/400, Solaris, NT/2000, z/OS. Tight integration with DB2.	Association rules, classification, clustering, time series. Leader in bringing new technologies to industrial strength tools.

Product Name	Vendor	Tool Type	Platforms	Mining types
Clemetine	SPSS	Integrated tool suite	Client: Windows Server: NT/2000, Solaris, HP/UX, AIX	Neural Networks, Decision Trees, Clustering, Association Rules, Sequential Associations
Enterprise Miner	SAS Institute	Interactive model development.	Client: Windows Server: NT/2000, AIX, Compaq Digital UNIX, HP-UX, Solaris 2, MVS, Linux	Decision trees, neural networks, regression, clustering, time series, associations
CART, MARS	Salford Systems	High accuracy classifier	Windows. Unix, Linux, MVS, CMS	Decision tree, regression

A current and complete list of both commercial and public domain data mining software, organized by type of data mining, is maintained at the KDnuggets web site: http://www.kdnuggets.com/software/Product/technology status.

While data mining tools are commercially available, they are not adapted to intrusion detection. Current work on data mining for intrusion detection is in the research prototype state, and is often built on custom algorithms rather than commercial tools. Deployment will likely be through existing or new companies specializing in IDSs.

Technology Insertion

Data mining may prove to be a useful tool in the FAA environment for new insights into the NAS operations as well as for intrusion detection. For now, the marketplace does not offer COTS products that would serve the FAA; such products are several years away. This may be an interesting research area for the FAA.

Future of Data Mining

Data mining has a great deal of potential for improving IDSs. Data mining clearly can sift through vast amounts of data and provide useful and actionable information after a system or network attack, but a number of important and difficult tasks remain. A few of these are: finding only "interesting" anomalies, finding anomalies in real time, training predictive models on enough data to make accurate models, but not so much as to overly delay the deployment of improved rules, and finding the best ways to exploit and combine transaction data from a variety of sensors.

One area where data mining-based approaches will likely outstrip conventional IDSs is in system and user profiling. User profiling will generally catch the attacker after they have gained access to the system. However, detecting such intrusion allows auditing to ensure that data integrity has not been compromised.

Another area where data mining has an advantage over conventional methods is with anomaly detection. Data mining has been successful in fraud detection in the credit card and telecommunications industries. This success is likely to extend to network security--traffic patterns that are common at one site may represent unusual and suspicious behavior at another site, particularly with well-disguised attacks. The ability to adapt to individual site behavior gives data mining an advantage in such an environment.

2.4.3 Public Key Infrastructure (PKI)

A PKI is a set of infrastructure components and services (including authentication, integrity, confidentiality, and non-repudiation) dedicated to managing keys and public key certificates in order to provide security services for enterprise resources. However, a PKI should not be viewed merely as a technology, but as a security infrastructure that includes technology, policies, procedures, and people.

A PKI typically includes one or more Certification Authorities (CAs), Registration Authorities (RA), and directories. The CA is responsible for issuing certificates, managing them during their life cycle (including renewing and revoking them), and publishing the certificates and their status to a central repository (e.g., directories). The RA registers users and is responsible for verifying the user identities before authorizing the CA to issue the certificate. Directories provide the repositories for certificates, user information, and certificate validity for access by users and applications.

The most mature and widely used PKI-enabled applications are secure e-mail (using Secure/Multipurpose Internet Mail Extensions), secure Web server access (using Secure Sockets Layer or Transport Layer Security), Single Sign-On, and VPNs (using Internet Protocol Security [Ipsec]). PKIs are also being used to provide digital signatures for objects (e.g., forms and code) and to secure electronic commerce and business-to-business transactions across insecure networks. Organizations are deploying PKIs to support business drivers, such as cost savings (maintain a single security infrastructure for enterprise resources), interoperability (employ common mechanisms to promote secure interoperability across applications and with other enterprises), and enhanced security (provide security services for enterprise resources and uniform identity credentials for users).

A fundamental requirement for PKIs is the development of supporting policies and procedures. A Certificate Policy (CP) should be developed that defines roles and responsibilities, together with a Certification Practice Statement (CPS) that defines how the PKI will be implemented and managed to support the CP. One of the major purposes of the CPS is to describe how the PKI will be managed securely, especially since the PKI will provide cryptographic keys for users and applications. Certificate profiles that define the content of particular certificates also need to be developed. These are living documents that reflect changes in policy, in the evolution of PKI, and in the capabilities supported by emerging products.

<u>Strengths</u>

Applications using PKI offer a significant step forward in adding trust to the current business infrastructure:

- Flexibility: PKI's public key provides secure communication without prior arrangements.
- Broad support: As depicted in Figure 2.4, PKI supports all of the Technology Areas shown.
- Public/private keys: One of the fundamental principles that enable public key technology to function is that the public key component of the technology is distributed openly and that the private key does not have to be distributed or exposed, as is required in symmetric key distribution configurations.
- Potential: PKI has potential for enabling e-commerce on a large scale.

Technology Area \ Mechanism	User Name/ Password	Encryption	Firewall	Intrusion Detection System	Virtual Private Network	Public Key Infrastructure
Authentication	X		X		X	X
Access Control	X		X	X	X	X
Confidentiality		X			X	X
Integrity		X			X	X
Non-Repudiation						X

Figure 2.4 Technology Areas and Security Mechanism Support

Issues

- Infrastructure: Development and management of the necessary infrastructure for PKI is still a significant challenge.

PKI and PIN/passwords. The key characteristics of PIN/password and PKI are highlighted in Table 2.10. Typically, the PIN/password is managed by a central location. The user has to obtain and store the PIN/password at a central location. A PIN/password is unique for access to a service. As a result, the system scalability of a PIN/password method is limited. On the other hand, an individual can obtain a PKI certificate from a registration/CA. With the appropriate policy established, a strong binding is provided between the individual and public/private key pair. Ideally, with the proper infrastructure, a PKI user can use the certificate obtained from one service provider for all available services.

Today, many companies learn the functions and features of PKI technologies and determine its usefulness in their own business environment. Identifying and developing PKI-enabled applications are the main efforts of this phase. When the company is satisfied with the technology, it will probably select a suitable business partner and begin the use of PKI for two-way e-commerce. The expansion of the PKI to accommodate all business partners, and eventually a global e-commerce environment, remains a challenge.

Table 2.10 Comparison of PIN/Password and PKI

Characteristic	PIN/Password	PKI
Architecture	Centralized	Distributed
Features	None	• Data integrity • Authentication • Non-repudiation
Personal Identity	Moderate	Strong
Interoperability	None	Evolving
Management/Operation	Local scale	Global scale

Ongoing R&D

Identifying an interoperable trusted model among business entities and searching for an efficient transport mechanism to deliver the certificate status are two main ongoing PKI R&D efforts. Today, industry is deploying two PKI interoperability approaches:

- Single root anchor: Under the root anchor system, the trusted relationship between business entities is established through the trusted anchor. The root anchor must certify the business entity's certificate before it can carry out a business transaction. A root CA exists for the organization and issues certificates to all certificate authorities and users beneath it in the hierarchy.
- Cross certification: Cross certification is a technology that builds a bilateral trusted relationship between business entities. The trust model for the cross certificate approach assumes that as long as two business entities trust each other, they can conduct business transactions.

As more PKIs use cross certification to interconnect, there will be a rapidly expanding number of cross-certification agreements, and a bridge architecture becomes viable. CAs wishing to cross certify merely cross certify once with the bridge's CA or one of its authorities. Assurance levels are beginning to be featured in these systems that allow a user to validate a trust path at a predetermined level that has been subject to a rigorous check for integrity. Through the interconnection with a bridge, complete certificate chains can be created from a PKI user at one organization to a PKI user at another organization attached to the bridge. The Federal Bridge Certification Authority (FBCA) is a federal government implementation of the bridging system. Mapping assurance level, dynamically searching a certificate path, and validating the certificate status are still under research.

Leading Organizations

Table 2.11 lists the leading companies and institutes that are working on these projects, technologies, and standards. FBCA is a government-funded project. The National Security Agency (NSA) is developing an Entrust CA-based bridging system for DoD, while the GSA/Department of Treasury is deploying a federal government-wide bridging system using Mitretek Systems as the integrator.

The Simple Certificate Validation Protocol (SCVP) is a proposed IETF draft standard. It allows a client station to query the certificate path and certificate status from a server system. The Online Certificate Status Protocol (OCSP) allows the application to request a certificate status without downloading the entire Certificate Revocation List (CRL).

Table 2.11 Leading Companies and Institutes for PKI Technology

Project/Technology	Leading Companies and Institute
FBCA	NSA, GSA, Mitretek, Entrust
SCVP standard and toolkit	Valicert, VPN consortium
OCSP standard and toolkit	Verisign Inc., Baltimore Technologies

Table 2.12 Points of Contact

Organization	Contact Information
NSA Bridge Project	Dave Fillingham: dwfilli@missi.ncsc.mil, 410-854-4537
NIST PKI Technical Working Group	William Burr: William.burr@nist.gov, 301-975-2914 or 301-948-0279
ValiCert, Inc.	Ambarish Malpani: ambatrish@valicert.com, 650-567-5457
Federal PKI Steering Committee	Judith Spencer: Judith.spencer@gsa.gov, 202-708-7500
NIST PKI Technical Working Group	Tim Polk: tpolk@nist.gov, 301-975-3348 or 301-948-1233
VPN Consortium	Paul Hoffman: Paul.hoffman@vpnc.org

Product/Technology Status

Table 2.13 IETF Standards and Products Status

Product/Technology	**Status**
Simple Certificate Validation Protocol (SCVP) draft standard draft-ietf-pkix-scvp-03.txt	June, 2000
SCVP toolkit	Q2FY01
Delegated Path Validation draft standard draft-ietf-pkix-ocsp-valid-oo.txt	August, 2000
OCSP-x toolkit	N/A

Technology Insertion

As a technology, PKI could be inserted into the FAA environment today to provide security services. A key PKI requirement, which has proven to be a considerable challenge, is the infrastructure needed to make the security service successful. The FAA should carefully examine its authentication requirements to ensure that PKI is the best way to meet those requirements.

Future of PKI

The PKI market is expected to drive the secure transaction market over the next several years, and will require greater authentication than provided by the typical 4-6 digit PINs being used currently. Part of that greater authentication is expected to be provided by biometric systems. Both PKI and biometrics are expected to grow at a compounded annual growth rate of about 60% through 2004 [4].

The future of PKI is somewhat dependent on the infrastructure with which it operates and interfaces, such as an e-mail system. Non-homogeneous environments in particular present special challenges for PKI.

2.5 ISS Technology Area 5: Availability

Availability ensures that a resource is accessible and usable by any authorized principal; information and/or services are not being withheld in an unauthorized manner—and thus, are accessible when needed without undue delay.

In the FAA environment, availability of information is important to the 24/7 NAS operational environment. The FAA has used redundancy, diversity, self-healing systems, switching and routing, and back-up systems to provide protection against normal outages.

but should the use and dependency on COTS-based networked systems increase, the issue of availability must also consider protection against cyber attacks.

2.5.1 Denial of Service (DoS) Defense

DoS attacks send large numbers of meaningless packets of data to a target system, such that the target system is flooded with so much traffic that legitimate traffic is slowed or halted, i.e., denied. DoS attacks are limited today to the Internet. FAA operational systems are not connected to the Internet. FAA administrative systems are connected to the Internet via firewalls, so are theoretically vulnerable. DoS attacks only serve to slow down or disrupt connections, and do not hack into networks or systems. These packets are designed to disable or overwhelm the target system, often forcing a reboot. Often the source address of these packets is "spoofed," making it difficult to locate the real source of the attack. According to a May 24, 2001 *New York Times* article, about 4,000 web sites experience DoS attacks each week; most of these attacks are brief and have little effect on the target.

In the basic DoS attack, the most affected service is a Web server. The attacker sends a stream of connection requests to a server in an attempt to exhaust all memory or to consume all processor capacity in that server.

In a Distributed Denial of Service (DDoS) attack, there might be a single attacker, but the effect of the attack is greatly multiplied by the use of attack servers known as "agents" that are remotely controlled by the threat agent. An attacker may subvert a large number of machines over a period of time, and install custom attack software in them. At a predetermined time, or on a given signal, these machines all start to bombard the target site with messages. The subversion may be automated using methods similar to those in the Morris worm [26].

Once an attack has started it is very difficult to stop it. The Internet itself was not developed with built-in flow control, so prevention and detection have to occur at other locations, such as the ISP and the user location. So long as connecting networks have vulnerabilities, then opportunities are available for launching DoS and DDoS attacks.

The prevention and detection of DoS and DDoS attacks requires true Defense in Depth, i.e., a variety and combination of policies, procedures, and technologies. The technologies themselves are already available in the marketplace, and while some may continue to improve through research, commercial versions can be used today with good results.

For prevention of DoS and DDoS attacks, security best-practices provide one first line of defense. Included in these best-practices are password management – using strong passwords that are difficult to break – and configuration management, with particular emphasis on timely application of ISS updates. Another first line of defense is filtering software can help detect inbound as well as outbound transactions that may be designed to deny service on a target server. Firewalls, which may include hardware and software, can help identify attack traffic, but the firewalls must be configured properly and have up-to-date software.

For detection of DoS and DDoS attacks, IDSs can help detect when a DoS or DDoS attack has begun and, depending on the product, provide one or more forms of alerts. Once an attack has begun, well-defined procedures can help minimize damage. These procedures might include re-routing or containment steps, as well as communication with other organizations connected to the network whose machines are possible sources or targets.

Current Strengths

- Best-practices: Security best-practices are known and publicly available. These can often be implemented with less cost than acquisition of new tools.
- Available software: Defensive software, such as for ingress or egress filtering, is widely available.
- Use of firewalls: Firewalls, when well-configured, are a well-known safeguard, and the proper configuration management responses are well-documented.
- Use of IDSs: An IDS, when well-matched to system and organization goals and requirements, can be an effective tool in identifying the beginning of a DoS/DDoS attack and helping to minimize the effect on the system.

Current Issues

- Interdependency: The security of any network on the Internet depends on the security of every other network. The widely varying implementation of security measures is what often makes a distributed attack successful.
- Variety of attacks: There is a great variety of DoS attacks. Hardware, software, and the network can all be attacked, which requires multiple defenses to be in place.
- Speed of attacks: DoS and DDoS attacks can spread quickly once they have begun. If proper detection support is not in place to identify the beginning of an attack and deflect it, considerable damage can be done to a site in a short amount of time.
- Mutations: Mutations are easily and quickly created. This requires constant updating of procedures and tools to be prepared for each new attack.
- Multiple defenses needed: Many different safeguards are required to defend against an attack. While some safeguards, such as well-configured firewalls, can do much to identify and defend against an attack, system administrators cannot rely on single solutions to a multiple-pronged problem.

Ongoing R&D

Research related to DoS and DDoS can be found in the various components of defending against DoS and DDoS attacks, and of managing them once they occur. In particular, the reader is referred to Section 2.2.2 on Intrusion Detection and the resources listed below.

Leading Information Resources

- The Center for Education and Research in Information Assurance and Security provides information on vulnerabilities and patches: www.cerias.purdue.edu.
- The CERT Coordination Center has extensive information, including alerts, information on vulnerabilities, patches, etc., at their Web site: www.cert.org.
- The ICSA Web site includes links to resources, a firewall policy guide and some free tools: www.icsa.net.
- The Information Systems Security Association is a professional association with links for training, resources, tools, patches, anti-virus solutions, etc.: www.issa.org.
- The SANS Institute publishes vulnerabilities, resources for training, and tips for hardening OSs. It also has training programs: www.sans.org.
- Security Focus provides tools and a technically oriented digest of vulnerabilities in the Bugtraq section of their Web site: www.securityfocus.com.
- Dave Dittrich at the University of Washington has done some exceptional work in analyzing hacker DDoS tools: www.washington.edu/People/dad/.
- Technotronic.com has a section on DoS attacks with basic information on security and DoS topics: www.technotronic.com/denial.html. www.technotronic.com/denial.html

Technology Insertion

Many of the technologies for DoS/DDoS defense are mature and ready for use in the FAA environment today. These technologies include ingress or egress filtering software and firewalls. Part of the defense strategy includes best management practices, such as configuration management, keeping defensive software up to date, and strengthening passwords. These management steps should be used now, with any ISS technologies.

Future DoS/DDoS Technologies

Research for these future technologies is found in other sections of this document, in particular intrusion detection, firewall technology, and anti-virus tools. Focus for managing DoS and DDoS will be research in network protocols and infrastructure to implement real-time flow analysis and flow control, as well as understanding the nature of “choke points” on the Internet. Intruder tools are evolving and the future DoS and DDoS detection efforts will have to evolve as well.

2.5.2 Disaster Recovery and Contingency Planning

Disaster recovery and contingency planning are essential for mitigating the impact of a disaster or to prevent it from happening in the first place. Much of a disaster recovery planning initiative is common sense. The rest can be greatly simplified through simple to use tools and templates. However serious a disaster is, the amount of impact it has on an organization is in many cases directly related to how prepared that organization is in advance. A well-constructed contingency plan that is in place and rehearsed prior to a crisis can in many cases severely curtail or even eliminate down-time, injuries and loss of life, repair costs and other interruptions to normal operations in many cases.

The term *business continuity* refers to the activities required to keep an enterprise running during a period of displacement or interruption of normal operation. *Business continuity* has become the standard industry term for strategic activities such as “disaster recovery,” “high-availability planning,” “continuous-availability planning,” and “emergency preparedness.” For the purposes of this paper and within the overall category of risk management, Business Continuity Planning (BCP) includes “disaster recovery planning” and “contingency planning.”

The separate plans that generally make up a BCP include:

- <u>Disaster recovery plan</u>: to recover mission-critical technology and applications at an alternate site.
- <u>Business resumption plan</u>: to continue mission-critical functions at the production site through workarounds until the application is restored.
- <u>Business recovery plan</u>: to recover mission-critical business processes at an alternate site (sometimes this is called “workspace recovery”).
- <u>Contingency plan</u>: to manage an external event that has a far-reaching impact on the enterprise.

A BCP is used when there is a disruption to operations, and should cover the occurrence of the following events:

- Equipment failure
- Disruption of power supply or telecommunications
- Application failure or corruption of a database
- Human error, sabotage, or employee strike
- Attack by malicious code (viruses, worms, Trojans)
- Hacking other Internet attacks
- Social unrest or terrorist attacks

- Fire or other natural disasters (e.g., flood, earthquake, hurricane).

The process for developing a BCP consists of the following three steps:

- Conduct a business impact analysis: This first step of analysis includes risk analysis and recovery strategy.
- Create the plan: Once the analysis is complete, a planning organization within the company will be formed, generally made up of representatives of the different parts of the organization.
- Test and maintain the plan: Once the business continuity plan is prepared it is then subject to an ongoing process of rigorous testing and maintenance.

Business continuity software, consultants, and services. A BCP is a high-value, if not a high-maintenance, proposition. Business continuity embraces a broad spectrum of technologies: old and new, paper-based and electronic, manual and automated, individual and integrated approaches. An enterprise can fully or partially outsource its business continuity solution.

BCP requires expertise that may need to be supplemented with the use of software, consulting services, remote support services, and services from non-profit organizations. Software based BCP tools may be very useful for developing an integrated and thorough BCP solution. There are also companies that offer planning assistance and/or recovery assistance. In addition, there are several non-profit organizations that provide research on vulnerabilities, training of IS personnel, and reporting of incidents.

Software products. Selecting a BCP software package depends on the presence (or absence) of a current plan, existing contracts with business continuity consultants and services, the amount of in-house resources available for the process, and the degree of control local managers wish to retain. BCP software, at a minimum, provides the planning methodology. Some BCP software supports business continuity all the way through the communication and implementation phases. Since packages range from simple electronic checklists to complex client/server and Web applications, choosing a package may be fairly complicated.

Purchasing a BCP tool essentially provides outside expertise in a form that is more readily accessible than books and articles on BCP. Often, the in-house BCP team is too close to its environment to see the whole picture. The software package takes the role of an objective outsider that asks “Have you thought of this?” BCP tools also are key for managing changes to the plan due to the inevitable changes in human resources, assets, processes, facilities, and information systems. Maintaining plans requires continual diligence and rigorous procedures.

BCP service providers and BCP consultants. BCP consulting services provide process support, educational services, risk analysis, and audits. In addition, BCP service providers may support an enterprise by offering physical recovery assistance support in the form of remote data storage vaults, off-site backup and storage, and recovery centers. There are various types of BCP consulting services available, such as the following:

- Software and Consulting: Many service providers offer combinations of tactical consulting with BCP and management software, sometimes including full continuity management services and hot-site facilities.
- Hardware and Consulting: Hardware vendors may combine continuity planning consulting with rapid hardware replacement shipment, mobile-site delivery, or hot-site facilities.
- Internet E-Commerce Continuity and Consulting: Communications and networking vendors may offer high-availability networking and rapid recovery solutions with tactical consulting.
- Product-Independent Consulting: Consultants who provide analyses, audits, and tactical recommendations based upon such studies offer objectivity in the development of the specifications a company should use to select business continuity products and services.
- PC-Based Planning Tools: Virtually all hot-site vendors offer some form of PC-based disaster recovery plan development tool. In many cases (like consulting services), these packages are provided to a client organization as an enticement to acquire full hot-site services.

Disaster Recovery Assistance. Stand-alone considerations for offsite recovery remain a significant part of the continuity management strategy. Specific types of services (as listed below) may be combined to provide the exact coverage needed.

- Original Equipment Manufacturer Insurance: Hardware companies may offer a form of insurance guaranteeing that they will replace damaged computer equipment with a system of equal or greater processing capacity within a specified period of time. The insurance cost is usually six to eight percent of the monthly maintenance bill.
- Quick Ship: Most third-party leasing vendors provide guaranteed rapid shipment of replacement hardware as a recovery option. Customers pay a priority equipment search fee and the normal leasing charges plus a premium when they request shipment.
- Hot Site: A hot site is a fully equipped, operationally ready data center offering specific hardware platforms ready for almost immediate use when the service provider is notified of a disaster. A hot site has all the equipment needed for the enterprise to continue operation, including office space and furniture, telephone jacks, and computer equipment.
- Cold Site: A cold site is an empty, environmentally conditioned computer room with office space, telephone jacks, etc., ready for the computer equipment to be moved in. However, since the customer provides and installs all the equipment needed to

continue operations, it takes longer to get an enterprise in full operation after the disaster.

- Mobile Site or Porta-Site: *Mobile sites* are stand-alone units on mobile trailers. *Porta-sites* are transported to the facility and constructed on-site. The advantage of mobile sites is that they can be set up in a parking lot or other company area, bringing the work area to the end user.

Business continuity companies may also offer recovery assistance by providing remote data storage of critical information, such as off-site storage and electronic vaulting.

- Off-Site Storage: Depending on budget and geographical risks, off-site storage for backup data on tape or disk could be the building next door, a bank safety deposit box, or the branch office across town. A better choice is a secure, climate-controlled, fireproof media vault at a storage facility maintained by a commercial media storage provider.
- Electronic Vaulting (or Advanced Recovery Services): Data is sent directly from the subscriber site to the hot site. This increasingly employed service requires that a direct-access storage device (DASD) be dedicated to the subscriber, preventing the service from being shared with other subscribers. Often the remote mass storage is part of a Storage Area Network (SAN).

Guidance for Disaster Recovery and Contingency Planning. Various non-profit organizations exist that offer research, training, and tactical services for the purpose of preventing and/or reporting of incidents. Recognized and established guidance for developing disaster recovery and contingency plans exists in the form of reference documentation from the IETF, FIPS, and the Carnegie-Mellon Computer Emergency Response Team (CERT).

- IETF, *Site Security Handbook*
- Carnegie-Mellon Software Engineering Institute (SEI) Computer Emergency Response Team (CERT) Coordination Center, *Steps for Recovering from a UNIX or NT System Compromise*, http://www.cert.org/tech_tips/win-UNIX-system_compromise.html.
- Carnegie-Mellon SEI CERT Coordination Center, *Incident Reporting Guidelines*, http://www.cert.org/tech_tips/incident_reporting.html.
- Carnegie-Mellon SEI CERT Coordination Center, Responding to Intrusions, http://www.cert.org/security-improvement/modules/m06.html.
- FIPS PUB 87, Guidelines for ADP Contingency Planning, http://www.itl.nist.gov/fipspubs/.

Incident Response Support Organizations. The CERT/Coordination Center (CERT/CC) is a major reporting center for Internet security problems. The CERT/CC staff members provide technical assistance and coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions, and disseminate information to the broader community.

The NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration and was founded in 1901 as the nation's first federal physical science research laboratory. The IS arm of NIST is its CSRC. CSRC's work is grouped into five major categories: cryptographic standards and applications; security testing; security research/emerging technologies; security management and guidance; and outreach, awareness, and education.

The FedCIRC is the central coordination and analysis facility dealing with computer security related issues affecting the civilian agencies and departments of the Federal Government. FedCIRC's incident response and advisory activities bring together elements of the DoD, Law Enforcement, Intelligence Community, Academia and computer security specialists from Federal Civilian Agencies and Departments forming a multi-talented virtual security team.

The Forum of Incident Response and Security Teams (FIRST), brings together a variety of computer security incident response teams from government, commercial, and academic organizations. This coalition was formed to meet the needs of a growing number of government and private sector organizations around the globe to exchange information and coordinate response activities.

Table 2.14 lists these organizations along with their Internet URL. These organizations can assist in the contingency planning, employee training, and/or in response to an IS incident.

Table 2.14 Non-profit Organizations Supporting Disaster Recovery and Contingency Planning

Organization (ACRONYM)	URL
Computer Emergency Response Team/Coordination Center (CERT/CC)	http://www.cert.org
NIST/Computer Security Resource Center (CSRC)	http://csrc.nist.gov
FedCIRC (Federal Computer Incident Response Capability)	http://www.fedcirc.gov
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org

Current Strengths

With the increase of Internet threats and terrorism, every enterprise can expect to respond to one or more types of business interruptions, whether from natural or criminal causes. With the shift of the information infrastructure from centralized processing to distributed processing and client/server technology, data is now located across the enterprise. It is no longer sufficient to rely on information technologists and system administrators to secure the information.

- Available resources: There are many resources for obtaining guidance and direct support for contingency planning processes and services. There are incident response support organizations (e.g., CERT/CC), service providers, and disaster recovery assistance providers (e.g., cold sites, hot sites, mobile sites). Guidance for disaster recovery and contingency planning are provided by the IETF, FIPS and the Carnegie-Mellon CERT. Each of these types of resources is fully described in previous sections.
- Peripheral benefits: A BCP involves all executives, managers and employees, which provide an excellent means for increasing and improving communication paths among various levels within an organization. Increased assurance to stakeholders, managers, and employees are secondary benefits of disaster recovery and contingency planning.

Current Issues

- Maintenance: BCP planning requires continual evaluation and revision. Changes in equipment, policies, business partners, and service providers all impact a BCP. Revisions to the BCP may be motivated by an enterprise's encounter with an actual technical interruption or natural disaster. Once invoked, an existing BCP may demonstrate weaknesses and vulnerabilities. Maintenance is needed at all levels of the enterprise, as policies and technologies evolve.
- Resources for testing the BCP: A BCP needs to be exercised, validated, and reported. Testing, training, documenting results, and revising the BCP takes considerable resources and coordination (internal and external to the enterprise). But without testing, the plan may fall short of its intended goals.

Ongoing Research

The Business Continuity Institute (BCI) (http://www.thebci.org): The BCI was established in 1994 to provide opportunities to obtain guidance and support with seminars, conferences, glossary, and the BCI Forum. Its purpose is to promote BP standards.

DRI International (http://www.dr.org): DRI was founded in 1988 to provide a base of common knowledge in contingency planning.

Disaster Recovery Journal (http://www.drj.com): This journal provides a wide range of resources.

Technology Leaders in the Business Continuity Market

Several major BCP software providers have decades of experience in the continuity planning industry. These include IBM BRS, Comdisco, LBL Technology Partners, Strohl Systems Group, and SunGard. With the acquisition by SunGard of Comdisco's business continuity assets on November 15, 2001, SunGard has become a global leader in integrated IT solutions.

- IBM Business Continuity and Recovery Services (http://www.brs.ibm.com): This is a business unit within IBM Global Services that focuses on managing the comprehensive business implications of an interruption in processing rather than simply coping with the technical problems. Services include risk analysis and management, disaster avoidance, consultation, recovery centers, and a range of business continuity and planning services. In addition, IBM offers fully-equipped hot sites, recovery assessment and planning services, critical business process continuity services, risk management, and continuity advisory services and business continuity services. IBM performs all the tasks necessary to execute an IT recovery program in a test or recovery scenario.

- SunGard Recovery Services (http://recovery.sungard.com): SunGard recovery services provides business continuity services, including high-availability infrastructure/electronic vaulting services, hot and cold sites, recovery network services, and workgroup recovery. Facilities for business continuity and disaster recovery include fully equipped computer facilities with hot sites supporting multiple platforms. In addition, SunGard provides mobile data centers and cold sites for the installation of replacement equipment. SunGard also has BCP software, including *PreCovery* and *ePlanner*. SunGard *eSourcing* system specializes in complex managed hosting services, comprehensive system and network management services, high-performance Internet access and high-bandwidth networking.

- Strohl Systems Group (http://www.strohlsystems.com): Strohl Systems Group is another global leader in BCP software and services. Products include business impact analysis tools (*BIA Professional* software and *BIA Web-server* application), *LDRPS system*, *Incident Manager*, and the *Envoy Automated Notification System*.

- LBL Technology Partners' (http://www.drj.com): *LBL Contingency Planner* organizes resources that could be overwhelming into a manageable modular process. The LBL Contingency Planner system automates the plan development process and provides an effective method for maintaining the plan. The software is a knowledge-based system that has been developed by certified BCP experts.

- Business Protection Systems (BPSI) (http://www.businessprotection.com): BPSI offers disaster recovery and BCP software and services. *Business Protector Professional* is a powerful plan development tool designed specifically for the creation of risk reduction and business continuity plans. This fully relational database software can be used on a single workstation or on a Local Area Network (LAN) or a WAN. *Business Protector Gateway* is a web-based application specifically designed for leveraging the Internet's advantages.

The BCP services of the major vendors are summarized in Table 2.15. The vendors are listed in the first column and the types of BCP services and tools that they provide are indicated with an asterisk ("*") in the remaining columns.

Table 2.15 Business Continuity Vendors at a Glance

Business Continuity Vendors at a Glance (as of October 2001)							
	Full Service Consulting	Management Services	BCP Software	Hot Sites	Cold Sites	Offsite Data Storage	Hardware Quick Ship
IBM BRS[4]	*	*		*	*	*	*
SunGard	*	*	*	*			
Strohl	*		*				
LBL Technology Partners	*		*				
Business Protection Systems	*		*				

Product/Technology Status

The field of disaster recovery and contingency planning products and services is experiencing tremendous growth. As enterprises become more aware of their vulnerabilities and liabilities, they are re-evaluating their priorities towards protecting their assets as well as their reputations. Businesses are increasing their budgets and resources to ensure that potential damage will be contained in the event of a cyber or natural disaster.

BCP software products have stabilized. These products are primarily used to facilitate BCP management and operational processes. BCP is not a technology; it is an on-going process.

[4] IBM Business Recovery Services unit

Technology Insertion

While BCP is not a technology, there are mature and available products in today's marketplace to assist the FAA in BCP activities. The options that may be available will likely change over time as this market grows in response to the new awareness of system vulnerabilities. The FAA should ensure that contingency and disaster recovery plans are in place. Some of the products above may be useful for that purpose.

Future of Disaster Recovery and Contingency Planning Services

In the 1980s, the business continuity market focused on IT disaster recovery. The trend has changed to provide complete systems availability to include addressing customer need for multivendor integrated-stack solutions (IT infrastructure comprised of multivendor components of software and hardware that are integrated and customized) within a fast-moving, 24x7 globalized infrastructure. As high-tech systems migrate from the data center and into the workplace, backup systems and working areas are both needed.

Outsourcing of business continuity functions will increase due to the greater dependence on web applications and requirements for speedy recovery of lost services and/or essential information. For the foreseeable future, the definition of these services will be undergoing some change, from outsourced management of centralized discrete resources to remote access of shared protected and secured joint resources.

2.5.3 Vulnerability Assessment

A vulnerability is a weakness in a system's security scheme, exploitation of which by a threat, would negatively affect the confidentiality, integrity, or availability of the system or its data. Reducing the vulnerable aspects of a system can reduce the risk and impact of threats on a system. In order to help accomplish this risk reduction, tools that automate the vulnerability discovery process continue to be developed and marketed.

Related to intrusion detection, these batch-level vulnerability assessment products determine the configuration, structure, and attributes for a given system device. This data is then compared to a database of known security holes to help determine vulnerabilities. In contrast to intrusion detection products that monitor a device or network for malicious activity in real or almost real time, vulnerability assessment tools are generally used on a periodic basis.

The type and level of detail of information provided among vulnerability assessment tools can vary greatly. Although some can identify only a minimal set of vulnerabilities, others can perform a greater degree of analysis and provide detailed recommended countermeasures. More recently developed tools provide user-friendly front ends and sophisticated reporting capabilities.

Vulnerability assessment tools can be categorized as host-based or network-based:

- Host-based vulnerability products: These are software agents that are placed on a variety of systems ranging from large servers to PCs to examine their environment. This examination can determine potential system level vulnerabilities based on known vulnerabilities in the OS. These agents report to a centralized management system that can report on the status of all systems with agents across the network.
- Network-based products: These are software products placed on the network to scan and monitor the network. They take inventory of all devices and components within the network infrastructure. These devices/components, the network configuration, and the various versions of software controlling the network are then examined and compared to a database of known vulnerabilities based on attack signatures.

Current Strengths

- Provide system administrators with the ability to assess the risk level of all systems that have agents loaded
- Provide a good way to determine the state of the network
- Easy to install and trial
- Able to run a wide variety of attacks on a network and determine the network resilience to each attack.

Current Issues

- Host-based products require agent installation on a large majority of systems.
- Both host-based and network-based products take a snapshot of a network and do not provide a real time solution.
- A 100%-availability hot site can nearly double an organization’s computing budget.

Ongoing R&D

A primary focus of vulnerability assessment R&D is on research to understand and enhance the security utility of new vulnerability assessment related technologies while also working to identify and mitigate vulnerabilities.

A good source for ongoing research can be found at the NIST CSRC at the following URL: http://csrc.nist.gov/ , and the Purdue University CERIAS homepage located at: http://www.cerias.purdue.edu/. Listed below is an overview of the research ongoing at CERIAS and NIST:

- CERIAS: Cooperative Vulnerability database and vulnerability analysis: The vulnerability database and vulnerability analysis group at CERIAS is collecting and analyzing computer vulnerabilities for a variety of purposes, including the application of knowledge discovery and data mining tools to find non-obvious relationships in vulnerability data, the development of vulnerability classifications, and the development of tools to help generate intrusion detection signatures from vulnerability information.
- NIST: Network management and security testing: A number of advantages of using mobile code and mobile agent computing paradigms have been proposed. These advantages include: overcoming network latency, reducing network load, executing asynchronously and autonomously, adapting dynamically, operating in heterogeneous environments, and having robust and fault-tolerant behavior. Most of these advantages are applicable to narrow application areas and more work needs to be done to verify these claims and evaluate security-related concerns in an operational environment. The focus of this research is to evaluate these claimed advantages and determine the applicability/benefits of using mobile agents for intrusion detection in large-scale enterprise applications, high-speed networks, high-volume data management requirements, and highly distributed and heterogeneous environments.

Leading Organizations

Leading commercial organizations providing products within the vulnerability assessment market can be categorized according to the segment of the market they support. The tools currently on the market fall within one or more of the following classes:

- Simple Vulnerability Identification and Analysis: A number of tools have been developed that perform relatively limited security checks. These tools may automate the process of scanning TCP/IP ports on target hosts, attempting to connect to ports running services with well known vulnerabilities and recording the response. They also may perform secure configuration checks for specific system features (e.g., network file system configuration and discretionary access control settings). The user interface of these tools is likely to be command driven, and the reporting may include limited analysis and recommendations. These tools are likely to be freeware.
- Comprehensive Vulnerability Identification and Analysis: More sophisticated vulnerability analysis tools have been developed that are fairly comprehensive in terms of the scope of vulnerabilities addressed, the degree of analysis performed, and the extent of recommendations made to mitigate potential security risks. Many of these tools also provide a user-friendly graphical user interface.
- War Dialers: A war dialer consists of software that dials a specific range of telephone numbers looking for modems that provide a login prompt. The tools, at a minimum, record the modem numbers and login screen, but can be configured to attempt brute force, dictionary based, login attempts. The value to system administrators is that these tools automate the process of identifying potential back doors in a network.

- Password Crackers: These tools attempt to match encrypted forms of a dictionary list of possible passwords with encrypted passwords in a password file. This is possible because the algorithm used to encrypt the OS's passwords may be public knowledge. Generally, these tools would be run by an attacker/insider in order to acquire a higher privileged level after gaining access to the system. Password crackers can support system administrators by allowing them to verify compliance with password selection policies.
- Risk Analysis Tools: These tools typically provide a framework for conducting risk analysis, but do not actually automate the vulnerability identification process. They may include very large databases of potential threats and vulnerabilities along with a mechanism to determine, based on user input, cost effective solutions to mitigate risks. The vulnerabilities identified using a vulnerability analysis tool may be input to a risk analysis tool to assist in determining the overall risk to the system.

Table 2.16 lists some of the leading commercial organizations and products by vulnerability assessment market segment.

Table 2.16 Leading Commercial Organizations and Vulnerability Assessment Products

Company	Products	Description	Web Site URL
AXENT Technologies	Omniguard/ESM	Comprehensive Host Vulnerability Assessment	www.axent.com
AXENT Technologies	NetRecon	Comprehensive Network Vulnerability Assessment	www.axent.com
Internet Security Systems	System Scanner	Comprehensive Host Vulnerability Assessment	www.iss.net
Internet Security Systems	Internet and Database Scanner	Comprehensive Network Vulnerability Assessment	www.iss.net
NETECT Inc.	Netective	Simple Vulnerability Analysis	www.netect.com
Cisco Systems	Cisco Secure Scanner	Complex vulnerability analysis	www.cisco.com
L3 Network Security, LLP	Retriever	Comprehensive Network Vulnerability Assessment	www.l-3security.com
Network Associates	CyberCop Scanner	Comprehensive Network Vulnerability Assessment	www.nai.com
BindView	BvControl (HackerShield)	Simple Vulnerability Analysis	www.bindview.com

Product/Technology Status

The worldwide software market for vulnerability assessment products is estimated to be about $360M in 2001 and is expected to grow an average of 31% per year through 2004. The companies listed in Table 2.16 currently comprise over 90% of the total market share [27].

BindView, due to its purchase of Netect and an increased emphasis on risk and security management, was the market leader with a 30% share, mostly from host-based systems. Internet Security Systems was second with 28% of the market and was the leader in network based solutions. AXENT's host-based solution revenue placed the company third with 24% of the market.

Vulnerability assessment, like intrusion detection, antivirus, content filtering, blocking, scanning, and firewalls are generally no longer statically deployed and must be continuously updated to deal with an ever-changing threat environment. Meanwhile, customers are realizing that the value of the product is not only the scanning engine, but the update itself. Consequently, many companies are looking for ways to expand their update infrastructure and processes to include a variety of other scanning technologies.

Other market drivers include:

- Desire for system level security
- Desire to strengthen network reliability by preventing network level attacks, such as DoS
- Desire to run quality control procedures on policy changes made by system/network management or other products on system/network devices.

Technology Selection Considerations

1. Criteria that could be used to evaluate and compare vulnerability assessment technologies:

    - Adherence to an existing agency standard that details the specific tool that should be acquired
    - Existence of a certification or warranty by the vendor to perform in an acceptable manner
    - Hardware and software environments required by the tool
    - Ease of use or user friendliness of the tool
    - System administrative skills required to support the tool and what vendor support is available
    - Cost of the tool

2. Current performance considerations:

   - Cost of Vulnerability Assessment tools can range from zero for freeware to over ten thousand dollars for comprehensive tools with a license to scan an unlimited number of networks. Within that range, there are a variety of offerings in the one to several thousand dollars range providing for limited network scans.
   - There also exists a wide divergence in the ease of use and maintenance of vulnerability assessment tools, with newer tools generally providing a user friendly interface and sophisticated reporting capabilities.

3. Evaluation and testing considerations:

   - When considering the use of vulnerability assessment tools, it is important to consider their number and placement within the host system/network architecture. Host based tools require installation on a large number of systems, and network based tools must be placed at the appropriate nodes within the network to be effective.
   - It is also important that vulnerability assessment tools take a snap shot of the network, and therefore, when testing, their utility temporal differences in system and network states must be taken into consideration.

Technology Insertion

The FAA should be performing vulnerability assessments on a regular basis, and there are tools available in today’s marketplace to facilitate that assessment. Vulnerability assessment is a changing market, but the FAA should select today’s best tools for their environment and plan to upgrade as those tools improve.

Future of Vulnerability Assessment

Host-based vulnerability assessment software is forecast to provide increased scalability, and tighter integration with system management tools, network based vulnerability assessment systems, and security policy management products. This will be accompanied by the development of click-and-fix functionality, which enables products to find a vulnerability, offer a solution, and automatically download and install a patch. Also forecast is the adoption and adaptation of the antivirus update model for distribution of new threat signatures.

Future trends in network based vulnerability assessment software will encompass all the enhanced integration and functionality forecast for host based vulnerability assessment software. In addition, expect aggressive marketing of network scanning services by ISPs and falling product prices. These services will include:

- Network level tests that scan all known IP services and look for common vulnerabilities

- Reporting functions that provide the ability to rapidly discover changes from previous scans and allow summary reporting over used defined periods of time
- Consulting services to assist in resolving any security vulnerabilities discovered.

3. ISS Research and Development

Table 3.1 identifies organizations that are involved in R&D efforts relative to each ISS Technology. The table identifies the corresponding organization, and, where possible, the product, and a point of contact reference. The content of this table provides many references, but should not be considered all-inclusive.

Table 3.1 Summary of ISS Technology Research and Development

ISS AREA	ISS Technology	Organization	Product (Report)	Point of Contact
Authentication	**Biometrics**	The Biometric Consortium		www.biometrics.org
Verifies the identity of a principle.	Technologies for measuring and analyzing human body characteristics, especially for authentication purposes.			
	Status: Gaining some acceptance where strong authentication is required.	BHSUG Newsletter		
	Weaknesses: User acceptance, cost, reliability.	List of major research centers		www.dss.state.ct.us/digital/news16/bhsug16.html
				www.cerias.purdue.edu/coast/hotlist/education/research_centers.html
	General Research	University of Bologna, Italy	Biometric Systems Laboratory	http://bias.csr.unibo.it/research/biolab/bio_tree.html

ISS AREA	ISS Technology	Organization	Product (Report)	Point of Contact
Authentication	**Biometrics**	Center for Education and Research in Information Assurance and Security (CERIAS) - Purdue University		www.cerias.purdue.edu/programs2000.php
		Center for Identification Technology Research (CITeR) - A National Science Foundation (NSF)/ Industry/University Cooperative Research Center		www.csee.wvu.edu/citer/citer.htm
		European Cooperation in the field of Scientific and Technical Research (COST)		http://europe.eu.int/comm/research/cost-h.html
		Michigan State University Biometrics Research		http://biometrics.cse.msu.edu
		MIT Media Lab's Vision and Modeling Group		http://www-white.media.mit.edu/vismod/
		Ohio University Center for Automatic Identification		wysiwyg://25/http://webit.ent.ohiou.edu/autoid
	1. Finger scan	FBI: Introduction to Wavelets	FBI Fingerprint Compression	http://www.amara.com/IEEEwave/IW_fbi.html
		FBI	FBI Fingerprint Image Compression Standard	http://www.c3.lanl.gov/~brislawn/FBI/FBI.html
		MITRE	Image Quality Evaluation	http://www.mitre.org/research/mtf/

ISS AREA	ISS Technology	Organization	Product (Report)	Point of Contact
Authentication	**Biometrics**	University of Bologna	FVC200 Fingerprint Verification Competition	wysiwyg://49/http://bias.csr.unibo.it/fvc2000
		NIST Visual Image Group	NIST Image Group's Fingerprint Research	http://www.itl.nist.gov/iaui/vip/fing/fing.html
		Signal Processing Research Centre, Queensland University of Technology	Finger Analysis	http://www.sprc.qut.edu.au/research/fingerprint.html
	2. Voice/Speech	Telematics Application Programme of the European Union, and Switzerland's Office Federal de L'Education et de la Science	CAVE - The European Caller Verification Project	www.ptt-telecom.nl/cave
		NIST	NIST Speaker Detection Evaluation	ftp://jaguar.ncsl.nist.gov/speaker
		Preception Science Laboratory, University of California	Speech Research	http://mambo.ucsc.edu/psl/speech.html
	3. Handwriting	The Nottingham Trent University	Intelligent Recognition and Interactive Systems (IRIS)	http://www.doc.ntu.ac.uk/HAND/
		University of Maryland	Document Understanding and Character Recognition (DIMUND)	http://documents.cfar.umd.edu/

ISS AREA	ISS Technology	Organization	Product (Report)	Point of Contact
Authentication	**Biometrics**	Handwriting Recognition Group, Nijmegen Institute for Cognition and Information (NICI), Nijmegen University, The Netherlands	On-line handwriting recognition, Unser-interfacing in pen computers, Outline-based image search; The Unipen Project	http://hwr.nici.kun.nl/ http://hwr.nici.kun.nl/unipen/unipen-anim.html
		BS Biometric Systems	HESY The Signature Pad: Authentifizierung und eindeutige Willenserklarung	http://www.BS-BiometricSystems.com/Start_D.htm
	4. Face	Preception Science Laboratory, University of California	Facial Analysis and Facial Animation	http://mambo.ucsc.edu/psl/fanl.html http://mambo.ucsc.edu/psl/fan.html
		Face Recognition Technology (FERET) - DoD	Development and evaluation of facial recognition systems	http://www.dodcounterdrug.com/facialrecognition
		Microsoft Research Vision Technology Group	Visual recognition, understanding, and interaction	http://research.microsoft.com/research/vision
		The Face Recognition Home Page	pointers to variety of other resources	http://www.cs.rug.nl:80/~peterkr/FACE/frhp.html
	5. Eye scan			
	6. Hand/finger geometry			
	Smart Cards	Electronic Commerce Research Room	Focus in on e-business transactions	http://wilssonweb.com/cgi-bin/au/research/money/smart.htm

ISS AREA	ISS Technology	Organization	Product (Report)	Point of Contact
Authentication	**Smart Cards**	ISSE Department, George Mason University		http://www.isse.gmu.edu Dr. Ravi S. Sandhu sandhu@isse.gmu.edu
		U.S. Government		http://smart.gov
		Cambridge University Computer Laboratory, Pembroke Street, Cambridge CB2 3QG		Ross J. Anderson: ross.anderson@cl.cam.ac.uk
		Prasad's Electronic Commerce & Smart Cards Page		http://home.att.net/~s-prasad/ecsc.htm
Access Control Prevents unauthorized access to and unauthorized use of resources.	**Intrusion Detection System (IDS)** Software and hardware devices that automate the process of monitoring the events occurring in a computer system or network, analyzing them of signs of security problems Status: fine data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to management systems which may need to interact with them	Purdue University	"A Taxonomy of Security Faults," Coast TR 96-05; 1996 "An Architecture for Intrusion Detection using Autonomous Agents; PDF Format," Coast TR 98-05; 1998	http://www.cerias.purdue.edu/coast/coast-library.html http://www.cerias.purdue.edu/ http://www.cert.org/index.html http://www.cerias.purdue.edu/coast/

ISS AREA	ISS Technology	Organization	Product (Report)	Point of Contact
Access Control	**Intrusion Detection System (IDS)** Weaknesses: Scalability, high error rate, interoperability	IETF	“Defending a Computer System Using Autonomous Agents,” CSD-TR-95-022; Coast TR 95-02; 1995 “Vulnerability Testing of Software System Using Fault Injection,” Coast TR 98-02; 1998 “Intrusion Detection Message Exchange Requirements,” “The Intrusion Detection Exchange Protocol (IDXP)”	http://www.ietf.org/internet-drafts/draft-ietf-idwg-requirements-05.txt http://www.ietf.org/internet-drafts/draft-ietf-idwg-beep-idxp-01.txt
Confidentiality Ensures that sensitive or classified information is neither available nor disclosed to unauthorized parties.	**Encryption**	RSA Security IETF National Security Agency (NSA)	Standards	http://www.rsa.com http://www.ietf.org http://www/nsa.gov

ISS AREA	ISS Technology	Organization	Product (Report)	Point of Contact
Confidentiality	**Virtual Private Networks (VPNs)** (Also, see research for routers, firewalls and encryption)	Virtual Private Network Consortium (VPNC) National Science Foundation's (NSF) Advanced Networking Infrastructure and Research Division		http://www.vpnc.org http://www.cise.nsf.gov/anir/index.html
Integrity Ensures that data cannot be altered without detection.	**Public Key Infrastructure** Infrastructure components and services dedicated to managing keys and public key certificate. It includes technology, policies, procedures, and people. Status: Prototyped for S/MIME e-mail applications. Testing encryption, assurance level, and web applications. Weaknesses: Interoperability, scalability, and performance	NSA GSA NIST Department of Treasury	• DoD Bridge – A DoD PKI interoperability infrastructure project • FBCA - A PKI interoperability infrastructure project for federal government	dwfilli@missi.ncsc.mil Judith.spencer@gsa.gov William.burr@nist.gov tpolk@nist.gov http://csrc.nist.gov/pki/fbca/fpkipa_bylaws_20001012.pdf http://csrc.nist.gov/pki/fbca/FBCA_CP_20001227.doc http://csrc.nist.gov/pki/fbca/fbcaguide_20001207.pdf

ISS AREA	ISS Technology	Organization	Product (Report)	Point of Contact
Non-Repudiation Enables a recipient of a message to prove the identity of the source of the message, and do so to the satisfaction of an independent third party.	Non-repudiation: All products that provide confidentiality also provide non-repudiation. Non-repudiation requires a consistent internal architecture comprising (in general, at least): confidentiality (encryption), authentication, and integrity. See the appropriate ISS Areas and ISS Technologies.			
Availability Ensures that a resource is accessible and usable on demand by an authorized principal.	**DoS Defense** **Distributed DoS Defense** (Also, see Intrusion Detection)	Center for Education and Research in Information Assurance and Security, Purdue University	Information on vulnerabilities and patches	http://www.cerias.purdue.edu
		CERT Coordination Center	Alerts, information on vulnerabilities, patches	http://www.cert.org
		Information Systems Security Association	Links for training, resources, tools, patches, anti-virus solutions	http://www.issa.org
		SANS Institute	Publishes vulnerabilities, resources for training and tips for hardening OSs	http://www.sans.org

4. Candidate R&D Areas for FAA ISS Hard Problems

The FAA shares many of the same ISS concerns as other government organizations and private industry. The federal government as a whole is a smaller customer for IT than in previous years, and does not drive the IT market as it once did. To the extent that the FAA's ISS requirements can be met by the current marketplace, the FAA can take advantage of the R&D being spent in response to the larger customer base. In this scenario, the FAA can monitor the various ISS technologies and insert them as appropriate. This strategy may be particularly useful in the case of administrative systems, whose operations more closely resemble those of the larger marketplace.

The FAA's NAS operations, however, have requirements that may not be met by the current general ISS technology market place. These requirements are unique in their operational nature and possibly their scale. It is toward these requirements that the FAA should focus its ISS R&D efforts, influence, and funding. Some of these requirements can be found in the list of security "Hard Problems" as compiled by the Infosec Research Council [28]. The following areas are candidates for FAA R&D efforts. (These areas are not listed in any particular priority order.)

4.1 Architecture

There is interesting research of possible information architectures that would serve the FAA well in the future. Within an overall information architecture, the following areas could be goals of the overarching architecture or independent research areas:

- System visualization: The FAA needs to be able to have a real time way to visualize and understand the current state of the NAS information systems. The NAS is a very complex IT environment. If it were to come under attack, it is important to know that an attack is underway and which portions are negatively affected and to what extent. A visualization of the condition of the NAS IT environment will greatly help develop a response to the attack. One model of such a visualization is found at http://www.incidents.org, with a movie at http://www.dshield.org.
- Graceful degrading or shutdown: If the NAS IT environment comes under attack, the most effective response may be to move to a degraded mode of operations, rather than shutting down the system entirely. How that graceful system degradation should occur is an interesting and important – and hard – question.
- Dynamic reconfiguration: Related to a graceful shutdown or degraded operation is the notion of dynamically reconfiguring the IT resources to minimize the effect of the attack and to allow the maximum NAS operations to continue. Research in this area could include compartmentalization and various response options to assist with reconfiguration decisions.

- Reliable recovery: If the NAS comes under attack and some portions must be degraded or shutdown, then it is important to know how to bring portions back into operation once damage has been contained or repaired.
- Leverage smaller scale COTS products: A good information architecture could assist in identifying areas that need more security or less security applied to them. Areas that need more security can possibly take advantage of very strong security products that operate well in environments smaller than the total NAS. An architecture can help with the configuration management requirements of inserting niche products into the total environment.

4.2 Aircraft Communications and Security

Plans to provide digital messaging service to and from the flight deck, digital voice communications, broadcast of traffic and broadcast of weather information raise the issue of the necessary security required to provide such services. User authentication, confidentiality and replay prevention may be needed on the air/ground "hop" and may be needed within the ground infrastructure between the broadcast site and the ground end-system involved. However, applying industry solutions, used today, to the aviation environment is not at all straight forward.

- Aviation applications, such as voice and Controller-Pilot Data Link Communications require real time and near real time delivery. Security services in an environment that requires a limit on delay may be very expensive and consequently not acceptable to the FAA environment.
- Security guarantees, such as authentication, integrity or non-repudiation, in a broadcast environment have not been widely addressed by the computer industry.
- The use of public/private key or secret key systems in a digital voice environment is not well understood and may not even be possible, due to the different levels of accuracy required by the key and voice systems. The confidentiality and authentication requirements of public/private or secret key systems assume that any change in transit is an indication of tampering or error, in which case the data is rejected. In the digital voice environment it is very possible that an error has occurred, but the information is still intelligible. Voice communication relies on this fact to limit the amount of bandwidth used.
- The limited bandwidth of the air/ground "hop" severely restricts the security solutions possible, both in the amount of information sent and in the timeliness of the information.
- Security solutions will probably not be restricted to the FAA domain. Air carriers, international civil aviation agencies and the public will need to be involved. This can introduce some very large management issues regarding key distribution that must be solved. For example, the use of a PKI encompassing multiple enterprises has not

been successful to date, nor has industry adequately addressed the needs to provide such a system within a safety related context, in which timing is critical.

The assumption that industry infosec mechanisms apply to the aircraft environment is probably not correct. In the best case considerable (re)working of the industry mechanisms may be necessary. In the worst case completely new technical and/or procedural approaches need to be researched which take into account restrictions imposed by performance, cost and safety.

4.3 Public Key Infrastructure (PKI)

Rivest, Shamir, and Adleman of RSA fame created public key cryptography several years ago and in doing so, advanced the use of cryptography to commonplace in today's computers and communications systems. Previous cryptographic systems required the use of secret keys at each site where the encryption/decryption was to occur. Key distribution of the secret keys to each of the sites quickly grew to be untenable when more than just a few sites were involved, especially in the commercial world.

Public key cryptography appears to solve the key distribution problem, with the publishing of the public key. Anyone wishing to send someone a private message could obtain a copy of the public key of the intended recipient and use it to encrypt the message. This system works well for both sending confidential information and signing a message for authentication purposes. There are obvious applications in both FAA administrative and operational systems for such a process.

Source authentication is part of the key management problem. To provide assurances as to the validity of the sender, a certificate of authenticity signed by a trusted third party is provided along with the message. As a further check, the recipient either assumes the certificate to be valid if it has not been revoked or actively queries a CRL server for this information. Once it is determined or assumed the certificate is valid, the transaction continues.

The IETF and the IP suite through the use of IPsec provides strong support for public key cryptography. The FAA's Information System Security Architecture requires IPsec. One of the primary protocols used in key management, Internet Key Exchange (IKE), has known problems. The IETF has issued a moratorium on any further extensions to IKE while stating publicly that it will be replaced as soon as it can be reengineered.

A second area that is problematic for the use of PKI is the CRL. Because of the delay time of updates, the cost of implementing a fully certificated system, and problems with cross-domain certificates, research should be conducted to consider a NAS PKI that does not use a full certificate-based system but is still based on public key cryptography.

4.4 System Security Engineering

A research area not normally considered within the "technology" domain is system security engineering. This area is concerned with the challenge of ensuring that a system is well engineered from a security perspective. It is a recognized hard problem by the FAA, by the NIST, and other organizations. The problem domain includes identification of security requirements, architecture, design, testing, implementation, operations, and maintenance. The FAA has an ongoing research activity to apply the Common Criteria and the Protection Profile methodology to the security engineering of large IT systems. A NAS System Protection Profile Template has been developed as a model for use in the acquisition of NAS Systems. While still in its infancy, it has been recognized by the National Information Assurance Partnership (NIAP) as a potential recommended security engineering practice for the Federal Government. A NIST-sponsored workshop to promote the idea is planned for September 13, 2002.

4.5 ISS Technology Performance Considerations

These considerations include the following elements:

- Impact of ISS technologies, such as encryption, on the end-to-end performance requirements of the NAS. These requirements tend to be stringent, and research could help evaluate whether the "sum is equal to the parts" or if the "sum" is going to be greater than the parts when considering additions or changes of ISS technologies.
- Component failover, such as failure of a firewall or authentication server. Performance will likely be affected until the service can be provided in another way. How to recover and/or bring the system(s) back into full operation in a way that maintains acceptable performance is an area that could benefit from research.
- Access control mechanisms used in NAS operations must be highly reliable. Failure of these mechanisms in certain situations may be untenable. For example, if an Airway Facility technician is at a remote facility to perform maintenance, failure of the access control medium, (such as a smart card), to allow Maintenance Data Terminal (MDT) access would be unacceptable if it prevented the scheduled maintenance to be performed.

4.6 Staffing Constraints

Given the market-wide competition for strong technical staff, the FAA should research ways to deploy ISS technologies in a way that does not rely on large numbers of highly skilled ISS technical staff. For example, with some technologies, operational consolidation using fewer staff may be more practical. Another factor that might be important is the robustness of the diagnostic tools that come with a product, and make it easier for scarce resources to manage that product. Some of this research may be related to the architecture research, in terms of knowing which components of the overall ISS architecture have different security requirements. One possible scenario might even be to outsource portions of the ISS support.

5. Proposed Next Steps

This document presents a snapshot of information at a certain point in time. The target application environment – the FAA – is changing as well as the ISS technology marketplace. In this context, and to take advantage of the work in this document, the following next steps are proposed:

1. Disseminate this information to all FAA Lines of Business: In addition to simply providing this information, also provide points of contact for follow-up questions or support.

2. Champion FAA-Specific ISS R&D: Evaluate the proposed candidate ISS R&D areas and develop a refined set of FAA-specific ISS R&D that the FAA should champion. Championing could take the form of direct FAA funding, collaborating with appropriate research organizations to leverage FAA resources, or influencing research in industry or other organizations.

3. Build Layers of System Protection: Begin to identify and agree upon ISS threats to the FAA operations, either administrative or the NAS. Select the best combinations of commercially available ISS technologies that can be used to counter each FAA ISS threat. Develop a funding strategy and an implementation plan to begin an ongoing Layers of System Protection program.

4. Maintain ISS information: Keeping this document's information up to date will be a steady and ongoing effort. The paradox is that the information will not be useful unless it is up to date. To reduce the FAA burden, a collaborative maintenance effort could be established with one or more organizations with similar interests, with the resulting living document available to a wider audience.

References

1. Mehan, Daniel J., *Information Systems Security: The Federal Aviation Administration's Layered Approach*, Transportation Research Board National Research Council, November-December 2000, *TR NEWS -Transportation Security -Protecting the System from Attack and Theft*, Number 211.

2. Federal Aviation Administration, June 9, 2000, *Information Systems Security Program*, FAA Order 1370.82, Department of Transportation, Washington, D.C., http://www.faa.gov/aio/common/documents/HTMLfiles/1370_82-NEW.htm.

3. Mehan, Dr. Daniel and Marshall Potter, *Building Trustworthy Systems: An FAA Perspective*, 2001, *Software Technology News, Volume 4, Number 3: Federal Aviation Agency Issue*, Data & Analysis Center for Software, Rome, NY.

4. IDC, November 2000, *Biometrics Market and Forecast: The Future of Hardware Authentication?*, IDC Bulletin, Document No. 23260.

5. Christiansen, C., N. Freedman, C. Kolodgy, 2001, *Return of the Black Box: Firewall/VPN Security Appliances Unleashed*, IDC Bulletin 24797.

6. Burke, B., C. Christiansen, N. Freedman, C. Kolodgy, 2001, *Worldwide Internet Security Software Market Forecast and Analysis, 2001-2005*, IDC Bulletin 24773.

7. Newman, D., J. Snyder, and R. Thayer, June 24, 2002, “Technology Insider: Network-Based Intrusion-Detection Systems,” *Network World*.

8. Rubin, Aviel D., and Geer, Jr., Daniel E., “Mobile Code Security,” IEEE Internet (November-December, 1998), pp. 30-34.

9. Jansen, Wayne A., Guidelines on Active Content and Mobile Code, Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Special Publication 800-28, October, 2001.

10. Kristol, David, “HTTP Cookies: Standards, Privacy and Politics,” ACM Transactions on Internet Technology (November, 2001), Vol. 1, No. 2, pp. 151-198.

11. Bergel, Hal, “Caustic Cookies,” Communications of the ACM (May, 2001), Vol. 44, No. 5, pp. 19-22.

12. Bergel, Hal, “Hijacking the Web,” Communications of the ACM (April, 2002), Vol. 45, No. 4, pp. 23-27.

13. Lawton, George, “Invasive Software: Who's Inside Your Computer?,” Computer (July, 2002), Vol. 35, No. 7, pp. 15-18.

14. Finjan Software, “Products Overview,” 2 pp., “SurfinGate for E-Mail,” 2 pp., “SurfinGate,” 2 pp., “SurfinShield Corporate,” 2 pp., “SurfinGuard,” 3 pp., all 2002. Available from www.finjan.com.

15. Gordon, Jennifer, “Finjan, Inc., SurfinGate and SurfinShield,” Gartner Research, DPRO-90713, October 4, 1999, 6 pp.

16. Edwards, Mark Joseph, "CAGE 2.3," Windows and NET. Magazine, April, 1999. Information on Digitivity is available at www.digitivity.com.

17. Gibbs, Mark, "Digitivity's Cage: Putting Java Applets Behind Bars," IntraNet, September 22, 1997, 2 pp. Available from www.nwfusion.com.

18. Microsoft Corporation, "Microsoft Authenticode Technology," 2 pp., "Signing and Checking Code with Authenticode," 17 pp., "Introduction to Code Signing," 7 pp., "Frequently Asked Questions About Authenticode," 12 pp., and "Important Release Information," 2 pp., all 2002. Available from www.microsoft.com.

19. Computer Associates, "Computer Associates Announces eTrust Defense Solution Set," 2 pp., July 9, 2001. Available from www.ca.com.

20. Trend Micro, "InterScan AppletTrap: Eliminating Malicious Mobile Code," 15 pp., Trend Micro, August, 2001. Available from www.trendmicro.com.

21. Payne, Jeff, RST Chief Executive, quoted in RST, "Reliable Software Technologies Selected by DARPA to Develop Mobile Code Security Technology," Cigital Labs August 23, 1999, 2 pp. Available from www.cigital.com.

22. Ibid., p. 1.

23. DARPA, "Sandboxing Mobile Code Execution Environments," Cigital Labs, 1999. 2 pp.

24. Steele, Bill, "Microsoft Grant Support Computer Virus-Protection Research at CU," Cornell Chronicle, October 25, 2001, 1 p.

25. Webster's Ninth New Collegiate Dictionary, 1985, Merriam-Webster Inc., Springfield, Massachusetts.

26. Anderson, R., 2001, *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley and Sons, Inc.

27. Kolody, C., et al., 2001, *Gaining Control over Infrastructure: Intrusion Detection and Vulnerability Assessment*, IDC Bulletin 23718, http://www.idc.com.

28. National Scale INFOSEC Research Hard Problems List, INFOSEC Research Council, 21 September 1999, http://www.infosec-research.org/documents.html.

Bibliography

1. Adams, C., and S. Lloyd, 1999, *Understanding Public-Key Infrastructure–Concepts, Standards, and Deployment Considerations*, Macmillan Technical Publishing.
2. Allan, A., February 12, 2001, *Security Applications of Biometrics: Perspective*, Gartner Group Technology Overview, DPRO-95808, Gartner Group, Inc.
3. Anderson, R., 2001, *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley and Sons, Inc.
4. Bace, R., and P. Mell, February 2001, NIST Special Publication on Intrusion Detection Systems.
5. Bergel, Hal, "Caustic Cookies," Communications of the ACM (May, 2001), Vol. 44, No. 5, pp. 19-22.
6. Bergel, Hal, "Hijacking the Web," Communications of the ACM (April, 2002), Vol. 45, No. 4, pp. 23-27.
7. Burke, B., C. Christiansen, N. Freedman, C. Kolodgy, 2001, *Worldwide Internet Security Software Market Forecast and Analysis, 2001-2005*, IDC Bulletin 24773.
8. Charlie K., R. Perlman, and M. Speciner, 1995, *Network Security*, Prentice Hall.
9. Christiansen, C., et al., April 28, 2000, *Internet Security Software Market Forecast and Analysis, 2000-2004*, IDC Software Research Database, http://www.idc.com.
10. Christiansen, C., N. Freedman, C. Kolodgy, 2001, *Return of the Black Box: Firewall/VPN Security Appliances Unleashed*, IDC Bulletin 24797.
11. Computer Associates, "Computer Associates Announces eTrust Defense Solution Set," 2 pp., July 9, 2001. Available from www.ca.com.
12. DARPA, "Sandboxing Mobile Code Execution Environments," Cigital Labs, 1999. 2 pp.
13. Edwards, Mark Joseph, "CAGE 2.3," Windows and NET. Magazine, April, 1999. Information on Digitivity is available at www.digitivity.com.
14. FAQ: Network Intrusion Detection Systems, TICM, March 2000.
15. Federal Aviation Administration, June 9, 2000, *Information Systems Security Program*, FAA Order 1370.82, Department of Transportation, Washington, D.C., http://www.faa.gov/aio/common/documents/HTMLfiles/1370_82-NEW.htm.
16. The Federal Information Processing Standard Publication 140-2 (FIPS PUB 140-2), *Security Requirements for Cryptographic Modules*.
17. Finjan Software, "Products Overview," 2 pp., "SurfinGate for E-Mail," 2 pp., "SurfinGate," 2 pp., "SurfinShield Corporate," 2 pp., "SurfinGuard," 3 pp., all 2002. Available from www.finjan.com.
18. Gibbs, Mark, "Digitivity's Cage: Putting Java Applets Behind Bars," IntraNet, September 22, 1997, 2 pp. Available from www.nwfusion.com.

19. Gordon, Jennifer, “Finjan, Inc., SurfinGate and SurfinShield,” Gartner Research, DPRO-90713, October 4, 1999, 6 pp.

20. Graubart, R. D., November 2000, *Biometrics: A Status Report on Emerging Technology*, MTR 00B0000048, The MITRE Corporation, McLean, VA.

21. IDC, November 2000, *Biometrics Market and Forecast: The Future of Hardware Authentication?*, IDC Bulletin, Document No. 23260.

22. Internet Engineering Task Force, September 1997, FYI-8/RFC-2196, *Site Security Handbook* (Section 5, “Security Incident Handling”).

23. Jackson, K., June 1999, *Intrusion Detection System (IDS) Product Survey,* Los Alamos National Laboratory.

24. Jansen, Wayne A., Guidelines on Active Content and Mobile Code, Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Special Publication 800-28, October, 2001.

25. Kohnfelder, L., May 1978, *Towards a Practical Public-Key Cryptosystem*, Bachelor’s Thesis, Massachusetts Institute of Technology.

26. Kolody, C., et al., 2001, *Gaining Control over Infrastructure: Intrusion Detection and Vulnerability Assessment*, IDC Bulletin 23718, http://www.idc.com.

27. Kristol, David, “HTTP Cookies: Standards, Privacy and Politics,” ACM Transactions on Internet Technology (November, 2001), Vol. 1, No. 2, pp. 151-198.

28. LaPadula, Leonard J., MITRE paper, Compendium of Commercial and Government Tools And Government Research Projects.

29. Lawton, George, “Invasive Software: Who’s Inside Your Computer?,” Computer (July, 2002), Vol. 35, No. 7, pp. 15-18.

30. Mehan, Daniel J., *Information Systems Security: The Federal Aviation Administration’s Layered Approach,* Transportation Research Board National Research Council, November-December 2000, *TR NEWS -Transportation Security - Protecting the System from Attack and Theft*, Number 211.

31. Mehan, Dr. Daniel and Marshall Potter, *Building Trustworthy Systems: An FAA Perspective*, 2001, *Software Technology News, Volume 4, Number 3: Federal Aviation Agency Issue*, Data & Analysis Center for Software, Rome, NY.

32. Menezes, A. J., P. C. van Oorschot, and S. A. Vanstone, 1996, *Handbook of Applied Cryptography*, CRC Press.

33. Microsoft Corporation, “Microsoft Authenticode Technology,” 2 pp., “Signing and Checking Code with Authenticode,” 17 pp., “Introduction to Code Signing,” 7 pp., “Frequently Asked Questions About Authenticode,” 12 pp., and “Important Release Information,” 2 pp., all 2002. Available from www.microsoft.com.

34. National Scale INFOSEC Research Hard Problems List, INFOSEC Research Council, 21 September 1999, http://www.infosec-research.org/documents.html.

35. Newman, D., J. Snyder, and R. Thayer, June 24, 2002, "Technology Insider: Network-Based Intrusion-Detection Systems," *Network World*.

36. Northcutt, S., 1999, *Network Intrusion Detection: An Analyst's Handbook*, New Riders.

37. Payne, Jeff, RST Chief Executive, quoted in RST, "Reliable Software Technologies Selected by DARPA to Develop Mobile Code Security Technology," Cigital Labs August 23, 1999, 2 pp. Available from www.cigital.com.

38. Portfolio Development Processes For Information Systems Security (ISS) and Information Technology (IT) Program Planning Team (PPT), AIO-4 Research and Development (R&D) Executive Board (REB) Meeting, Tuesday, January 30, 2001 (Briefing).

39. Potter, M., February 21, 2001, FAA Information Systems Security (ISS) Research and Development (R&D) Requirements, AIO-4, (Briefing).

40. RFC2828, Internet Security Glossary.

41. Rubin, Aviel D., and Geer, Jr., Daniel E., "Mobile Code Security," IEEE Internet (November-December, 1998), pp. 30-34.

42. Schneider, F., ed., 1999, National Research Council, *Trust in Cyberspace*, National Academy Press, Washington, DC.

43. Schneier, B., 1996, *Applied Cryptography*, 2nd Edition, John Wiley & Sons, Inc.

44. Stallings, W., 1998, *Cryptography and Network Security, Principles and Practice*, 2nd Edition, Prentice Hall.

45. Steele, Bill, "Microsoft Grant Support Computer Virus-Protection Research at CU," Cornell Chronicle, October 25, 2001, 1 p.

46. Trend Micro, "InterScan AppletTrap: Eliminating Malicious Mobile Code," 15 pp., Trend Micro, August, 2001. Available from www.trendmicro.com.

47. Warwick F., 1994, *Computer Communications Security*, Prentice Hall.

48. Webster's Ninth New Collegiate Dictionary, 1985, Merriam-Webster Inc., Springfield, Massachusetts.

Appendix A. ISS Technology Products and Sources

Table A.1 presents a snapshot of some ISS products available at the time of the writing of this document. Because ISS is a growing and very active marketplace, this table should not be considered complete. Inclusion on this table does not represent an endorsement of any product.

Column 1 indicates one of the five major FAA ISS technology areas of security services/functions.
Column 2 indicates ISS technologies that support the ISS technology area in column 1.
Column 3 indicates some leading organizations related to the respective ISS technology area or ISS technologies.
Column 4 indicates specific ISS product information of organizations in column 3.

Table A.1 Summary of ISS Technology Products

ISS AREA	ISS Technology	Company	Product	Point of Contact
Authentication Verifies the identity of a principal.	**Biometrics** Technologies for measuring and analyzing human body characteristics, especially for authentication purposes. Status: Gaining some acceptance where strong authentication is needed. Weaknesses: Cost, reliability, and concerns for privacy.	Vendors shown below will be in descending order by their share of their market segment as of 1999. DoD has established the Biometrics Fusion Center, a biometrics testing laboratory to scientifically scrutinize nearly 600 commercial products that scan unique physical traits and determine if any are good enough for widespread—and possibly mandatory—use by DoD. The Biometric Consortium	Finger scan, voice authentication and signature verification are the three fastest-growing segments by sales. There are no plans to release the test findings, but the Biometrics Fusion Center hopes to make recommendations to the Pentagon's upper echelons on the use of biometrics that could lead to large-scale purchases.	www.biometrics.org

ISS AREA	ISS Technology	Company	Product	Point of Contact
Authentication	**Biometrics**	Assoc. for Biometrics International Biometric Industry Association		www.afb.org.uk www.ibia.org
	1. Finger scan	Software/hardware:		
		Identix	- Identix BioTouch PC Fingerprint Reader - DFR 200 and DFR 300 fingerprint readers - Datawise MT Digit - Key Tronic Secure Scanner Keyboard - Bio Logon 2.0 Suite	www.identix.com
		Sagem		www.sagem.com
		Veridicom	- 5th Sense - SDK Software Development Kit - VBX 110 BIOS Development Kit - Secure Start & Secure Suite from I/O - Private Web - FPS110, FPS 200 - Protector Suite	www.veridicom.com
		Infineon	SAM	www.infineon.com
		Chips: Motorola ST Microelectronic ThomsonCSF		

ISS AREA	ISS Technology	Company	Product	Point of Contact
Authentication	**Biometrics**	Algorithms: NEC		
	2. Voice authentication	T-Netix	SpeakEZ VoicePrint	www.t-netix.com
		ITT		www.itt.com
		Nuance	- Nuance 7.0 - Nuance Verifier 2.0 - Nuance Voyager	www.nuance.com
		Veritel		www.us.veritel.com
	3. Signature verification	Communication Intelligence Corporation (CIC)	- ISign - Sign-it - Sign-On for Palm - Sign-On for Pocket PC	www.cic.com
		Cyber-SIGN	Cyber-SIGN	www.cybersign.com
		PenOP		www.penop.com
	4. Facial scan	Visionics	FaceIt Face Recognition Technology	www.visionics.com
		Viisage	- FacePASS - FaceADVISOR - FaceEXPLORER - FacePIN - FaceNET - FaceFINDER - FaceTOOLS	www.viisage.com
		eTrue	- TrueFace Engine - TrueFace ID	www.etrue.com
	5. Eye scan	Iridian Technologies, Inc.	- PC Iris - Private ID	www.iriscan.com
	6. Hand/finger geometry	Recognition Systems	Recognition Systems HandReaders	www.recogsys.com

ISS AREA	ISS Technology	Company	Product	Point of Contact
Authentication	**Biometrics**		- HandPunch family - HandKey family	
Access Control Prevents unauthorized access to – and unauthorized use of – resources.	Access Control List	Systems Advisory Group Enterprises CyberSafe	BRICKHouse Secure Web Server CyberSafe - Products	www.sage-inc.com www.cybersafe.com
	Firewalls	Hardcastle Electronics	F-Secure	www.helec.co.nz
	Authentication-based	Intracept Hpinet Secure Pilot	Intracept - X-Ray Vision Identikey (Java over SSL) SecurePilot (Palm Pilot based)	www.intracept.com www.hpinet.com www.securepilot.com
Integrity Ensures that data cannot be altered without detection.	Multi-Function (encryption, authentication integrity, etc.)	Cryptoengine	Global Encryption Technology Products	www.cryptoengine.com
Confidentiality	Cryptography	Network Associates	PGP Corporate Desktop - Single desktop solution combining personal firewall, intrusion detection, VPN client, and encryption technologies that fully protects computers against intruders and theft/loss of data	http://www.pgp.com/products/dtop-security/default-encryption.asp

ISS AREA	ISS Technology	Company	Product	Point of Contact
Confidentiality	Cryptography	Network Associates	PGP Keyserver - A comprehensive security infrastructure that incorporates public-key cryptography, certificates, digital signatures and encryption	http://www.pgp.com/products/keyserver/default.asp
		Baltimore Inc.	Mailsecure - A full set of security functions to be added to e-mail systems	http://www.baltimore.com/securityapplications/mailsecure/index.html
		Baltimore Inc.	Mailsecure Enterprise - Centralized e-mail security for the organization	http://www.baltimore.com/securityapplications/mailsecure-enterprise/index.html
		Baltimore Inc.	Formsecure - a security framework that lets you, build public key cryptographic security into any of your Web forms and so allow many people to digitally co-sign and secure data for web transmission	http://www.baltimore.com/securityapplications/formsecure/index.html
		Baltimore Inc.	Filesecure - FileSecure takes all incoming objects, which may be presented as files or e-mail, secures them, and then presents them either to be sent out, collected or stored	http://www.baltimore.com/securityapplications/filesecure/index.html

ISS AREA	ISS Technology	Company	Product	Point of Contact
Confidentiality	Cryptography	Baltimore Inc.	Websecure - WebSecure is a system designed to enhance almost any web server to browser communication to provide full 128-bit encryption for real security	http://www.baltimore.com/securityapplications/websecure/index.html
		F-Secure	VPN+ - F-Secure VPN+ secures the transmission of mission critical data over TCP/IP networks, such as the Internet	http://www.f-secure.com/products/vpnplus/
		F-Secure	SSH - F-Secure SSH Client and Server enable remote systems administrators and telecommuters to access corporate network resources without revealing passwords and confidential data to possible eavesdroppers. It protects TCP/IP-based terminal connections in UNIX, Windows and Macintosh environments	http://www.f-secure.com/products/ssh/
		RSA Security	BSAFE - A suite of core level cryptography tools allowing for the incorporation of cryptography into products	http://www.rsasecurity.com/products/bsafe/index.html
		Crypto AG	Infoguard AG - A suite of cryptography based security solutions for commercial business	http://www.crypto.ch/crypto_flash/business.html

ISS AREA	ISS Technology	Company	Product	Point of Contact
Confidentiality	Cryptography	IBM	PCI Cryptographic Coprocessor - The IBM PCI Cryptographic Coprocessor adds a high-security environment to OS/2, Windows NT, Windows 2000, AIX, OS/400, z/OS, and OS/390 server systems for DES, RSA, and DSA cryptographic functions and sensitive custom applications	http://www-3.ibm.com/security/cryptocards/index.shtml
		IRE	Safenet VPN - A suite of crypto based security products for government and industry	http://www.safenet-inc.com/index.asp
		Information Security Corp.	DSA Signature Software - Developed by ISC and licensed by AT&T, DSA Signature Software verifies the integrity of electronic documents.	http://www.infoseccorp.com/products/dsa.htm
Availability Ensures that a resource is accessible and usable on demand by any authorized principal.				

ISS AREA	ISS Technology	Company	Product	Point of Contact
Non-repudiation Provides proof that a message was sent or received.	All products that provide confidentiality also provide non-repudiation. Non-repudiation requires a consistent internal architecture comprising (in general, at least): confidentiality (encryption), authentication, and integrity. See the appropriate ISS Areas and ISS Subareas			

Acronyms

AFB	Association for Biometrics
ATC	Air Traffic Control
AV	Anti-virus
BC	Biometric Consortium
BCI	Business Continuity Institute
BCP	Business Continuity Planning
CA	Certification Authority
CERT	Carnegie-Mellon Computer Emergency Response Team
CIC	Communication Intelligence Corporation
COTS	Commercial Off-the-Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSRC	Computer Security Resource Center
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DoD	Department of Defense
DoS	Denial of Service
DSL	Digital Subscriber Line
EPROM	erasable programmable read only memory
FAA	Federal Aviation Administration
FBCA	Federal Bridge Certification Authority
FedCIRC	Federal Computer Incident Response Center
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GSA	General Services Administration
IBIA	International Biometric Industry Association
IBM	International Business Machines
ICC	integrated circuit chip
ICSA	International Computer Security Association
IDS	intrusion detection system
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
IS	Information Security
ISO	International Organization for Standardization
ISP	Internet Service Provider

ISS	Information Systems Security
ISSE	Information Systems Security Engineering
IT	Information Technology
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
NAS	National Airspace System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSF	National Science Foundation
OCSP	Online Certificate Status Protocol
OGP	Office of Government-wide Policy
OS	operating system
OSI	Open Systems Interconnection
PC	personal computer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RA	Registration Authorities
RAM	random access memory
R & D	Research and Development
ROM	read only memory
RSA	Rivest-Shamir-Aldeman
SCVP	Simple Certificate Validation Protocol
SMTP	Simple Mail Transfer Protocol
UK	United Kingdom
URL	Uniform Resource Locator
VPN	Virtual Private Network
VPNC	Virtual Private Network Consortium
WAN	Wide Area Network
WWW	World Wide Web

Glossary

Access control: The collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system.

Authentication (also **Identification**): Process to establish a user's identity prior to allowing general network access. While authentication can be as simple as typing in a user name and password, more sophisticated techniques utilize smart cards or biometric identification and authentication.

Authorization: More granular than authentication, authorization is a process for granting access to specific applications or data based on the user's role within the organization.

Availability: Property of system that measures the ability of that system to be used on demand by authorized users, usually expressed as a percentage. The gold standard is 99.999% availability.

Biometric identification: Authentication of users by unique biological characteristics, such as fingerprint, facial retinal, iris or voice patterns.

Certificate authority (CA): A server, managed either in-house or by a third party, that provides digital certificates to authenticated users.

Confidentiality: The ability to transmit or store information so that it cannot be understood except by the intended recipient or authorized user.

Cryptography: The science and technology of establishing or protecting the secrecy, authenticity, or integrity of data that might be accessed by unauthorized parties by using a code or cipher.

Data integrity: The ability to prevent transmitted data from being modified, including writing, changing, deleting, or replacing the original data or its descriptors.

Denial of service (DoS): An attack on an Internet connection that inundates a Web server with too many requests causing it to be unresponsive.

Digital Certificate: An electronic file used to authenticate users of a Public Key Infrastructure that includes a variety of information including personal information (such as name and e-mail address of the user), the company issuing the certificate, and the period during which the certificate is valid as well as encryption keys and digital signatures (see Certificate Authority).

Digital signature: A means of proving that a file was authored by a specific person.

Encryption: A process for scrambling (encrypting) and unscrambling (decrypting) electronic files into an unreadable format using a mathematical algorithm.

Firewall: A defensive mechanism typically deployed at the boundary between a trusted and a mistrusted computer network. Firewalls filter network traffic to allow only valid transmissions into internal networks.

Hacker: Someone who intentionally breaches computer security.

Identification: See Authentication

Integrity: The assurance that data have not been altered from their source without detection. This includes accidental or malicious modification, alteration or destruction.

Intrusion Detection: Real-time and reactive analysis of network usage patterns to detect abnormalities indicative of hackers, such as exceptional traffic from unusual locations or a single IP address.

Mobile Code: Code that is sourced from a remote, and possibly untrusted, system but executed locally. Other names for mobile code are mobile agents, downloadable code, executable content, active capsules and remote code.

Non-repudiation: Ability to provide proof that a transaction actually occurred between two specified parties.

Public Key Infrastructure (PKI): Encryption protocol that relies on a Certificate Authority to distribute digital certificates containing public key-private key pairs to authenticate and sign electronic transmissions.

Secure Multipurpose Internet Mail Extension (S/MIME): An extension to the industry standard MIME protocol that defines how an e-mail message is encoded and decoded. S/MIME messages include not only the message itself but also the sender's digital certificate.

Secure Sockets Layer (SSL): A transmission security standard developed by Netscape Communications to enable secure commercial (e.g., credit card) transactions to take place over the Internet. Utilizing private key-private key encryption, it creates a secure relationship between the client and server allowing server authentication, data encryption and data integrity.

Smart Card: A card about the size of a credit card embedded with a microchip that can store and process data. These cards can hold digital certificates or other information used for two-factor authentication.

Token: An authentication device used to generate one-time passwords or to participate in challenge/response authentication processes. Tokens may be small, handheld hardware devices similar to pocket calculators or credit cards.

Virtual Private Network (VPN): Use of a secure transmission protocol such as SSL for communication between two computers over public networks to ensure that data transmissions are not intercepted by unauthorized parties.

Virus: A self-replicating code segment that attaches itself to ordinary files. Commonly transmitted through e-mails and downloadable software, viruses range from annoying pranks to programs that destroy files or entirely disable computers.

Vulnerability: A weakness in a system's security scheme, exploitation of which by a threat would negatively affect the confidentiality, integrity, or availability of the system or its data.